OfficeConnect® Remote 812 ADSL Router CLI User's Guide

Release 2.0

http://www.3com.com/

Part Number 10043337 AA

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with this User's Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, and OfficeConnect are registered trademarks of 3Com Corporation. OfficeConnect Remote 812 is a trademark of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

Artisoft and LANtastic are registered trademarks of Artisoft, Inc. Banyan and VINES are registered trademarks of Banyan Systems Incorporated. CompuServe is a registered trademark of CompuServe, Inc. DEC and PATHWORKS are registered trademarks of Digital Equipment Corporation. Intel and Pentium are registered trademarks of Intel Corporation. AIX, AT, IBM, NetView, and OS/2 are registered trademarks and Warp is a trademark of International Business Machines Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. PictureTel is a registered trademark of PictureTel Corporation. UNIX is a registered trademark of X/Open Company, Ltd. in the United States and other countries.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Table of Contents

1

ACCESSING THE CONFIGURATION INTERFACE

2

CLI COMMAND CONVENTIONS AND TERMINOLOGY

3

CONFIGURATION METHODS

4

QUICK SETUP

5

QUICKVC SETUP

6

MANUAL SETUP

1 ACCESSING THE CONFIGURATION INTERFACE

This chapter explains how to attach to the configuration interface locally via the console port or remotely via a Telnet session. This chapter also introduces you to the capabilities and conventions associated with management of your OfficeConnect® Remote 812.

Establishing Communications with the OfficeConnect Remote 812

Local Connection

If you want to attach locally to the OfficeConnect Remote 812 (also referred to hereafter as the OCR 812) via the console (serial) port, you will need to connect the supplied serial cable to the Console Port located on the unit and the Serial Port on your computer. In addition, you will also need a terminal emulation program appropriate for your computer. See the following subsections for various emulation options.

No matter which emulator you use, configure your settings to:

- 9600 baud
- 8 data bits
- no parity
- 1 stop bit
- direct connect

IBM-PC Compatible Computers

Windows Terminal (included with Microsoft Windows) and ProComm Plus are popular communications packages which support VT100 terminal emulation for IBM-PC compatible computers. HyperTerminal, bundled with Windows 95, also provides terminal emulation.

Macintosh Computers

ProComm, MicroPhone, White Knight, Kermit, Red Ryder, VersaTerm and ZTerm (a shareware application available on the Internet and many online services) are popular communications programs which carry vt100 terminal emulation service for Macintosh computers. If you don’t have a communications package or your program doesn’t support vt100 emulation, ZTerm will function just as well.

UNIX-Based Computers

Kermit, minicom and tip are typical terminal emulation programs for UNIX-based computers. Depending on the platform you're using, you may need to modify a configuration file for vt100 settings.

Remote Connection

If you want to attach to the OCR 812 via the LAN or WAN interface of the unit, you will need to establish a Telnet connection to the unit.

The OCR 812 must have an IP address and an administrative login profile (username and password) in order to connect to it with Telnet. The IP address and administrative login profile are automatically created when the unit is initially configured using the IP Wizard or in DHCP Smart Mode. The default username is 'root' and the default password is '!root'. Refer to the OCR 812 ADSL Router Installation Guide for information on the IP Wizard or DHCP Smart Mode initialization. Alternatively, the IP address and administrative login profile can be created with CLI using the QuickSetup program or using individual commands.

From Windows 95, you can go to the DOS Window and run:

```
telnet <ip_address>
```

This will bring up the login prompt for the unit. Once you have successfully logged in, the Command Line Interface presentation is the same as if you were locally attached.

When you want to terminate your Telnet session, type ***quit*** *at the CLI prompt.*

2 CLI COMMAND CONVENTIONS AND TERMINOLOGY

This chapter describes the command syntax, conventions and terminology used within the Command Line Interface. Reviewing and understanding this chapter is essential for you to understand subsequent chapters.

Command Structure

Format

Commands can be followed by values and/or parameters and values. For example:

```
add ip network <network_name>
               address [ip_addr]
               { interface [eth:1] }
```

- **add ip network** is the command
- *<network_name>* is the (required) value for the command
- **address** is a required parameter
- *[ip_addr]* is the value for the IP address parameter which you must provide
- **interface** is only required if you want to override the default value, which is eth:1

Parameters

- are order independent
- **{** … **}** parameters enclosed by curly braces are required, and are provided with default values. You do not need to specify these parameters unless you wish to override the default.

Values

- **<** … **>** required values for a command or parameter are enclosed by arrows.
- **[** … **]** range of values following parameters are enclosed in brackets. Inside the brackets, if you see a:
  - **|** (vertical bar) you may select only *one* of the displayed choices: [FIRST **|** SECOND **|** THIRD]
  - **,** (comma) you can select *one or more* of the displayed choices: [FIRST,SECOND,THIRD,...]

- The type of value you enter must match the type requested. Numbers are either decimal or hexadecimal. Text can be either a string that you create, or it may be a list of options you must choose from. When choosing an option, type the text of the option exactly.

Names or Strings

- "Double quotation marks" set off user-defined strings. If you want white space or special characters in a string, it must be enclosed by "double quotation marks".

Network Address Formats

Many commands require a network address, to define a link to a remote host, workstation or network. Network addresses are shown in this document using the syntax described in the following table:

Address Type	Format	Range
IP_address	a.b.c.d	0.0.0.0 to 255.255.255.255 (decimal)
ip_net_address	a.b.c.d/mask	255.255.255.255/A,B,C,H
mac_address	xx:xx:xx:xx:xx:xx	hexadecimal digit pairs

Abbreviation and Command Completion

- Commands can be *abbreviated* if arguments you write are unique.
  For example, you can type **se vc jay pa bird**, short for: **set vc jay password bird** is acceptable, but **se vc jay i 222.111.111.111** isn't unique because **i** can stand for **ip, ip_routing,** or **ip_source_validation**.
- As a convention, some commands illustrated in this manual are abbreviated and annotated as such *(abbr.)* for brevity.
  Also*, s*ome parameters are omitted in examples because they default to standard values and do not require entry, or are unnecessary for common configuration. See the *CLI Reference* section for more details.
- *Command completion* finishes spelling a unique, abbreviated parameter for you just by pressing the key. It's handy when you're in a hurry or uncertain about a command. For example, if you type **add ip n[ESC]**, it will spell out the keyword **network** without losing your place in the command syntax.

Control Characters

- Commands can be *retrieved* by typing **<ctrl>p** [^p] (for previous) and **<ctrl>n** [^n] (for next). Command retrieval consults the *history* of previous fully entered commands, defaulting at the last ten commands.
- If an error occurs while a command is processing, any partial command (up to and including the field in error) is added to the history list.
- The current command can be *killed* by pressing **<ctrl>c** [^ c].
- A partially completed command line can be *reprinted* - a useful function if, due to interrupted output, you're unsure what the OCR 812 has "seen" up to now - by pressing **<ctrl>l** [^ l] (for last).

Help

Help is *general or positional*. Type **help <any command**> to get a cursory list of associated commands and its syntax. Type **<any command>?** to get more extensive, positional help for a particular field.

Help is most useful *during* configuration: query the list of possible parameters by typing **?** and, when you find the value you need, type it without losing your place in the argument. Just be sure to leave a space between the keyword and the question mark.

Conventions

- Most commands are *not* case sensitive. As a rule, only <*name*> and *[password]* values require typing the correct case.
- Configuration changes occur immediately **but are lost on reboot unless you save them.** The **save all** command places configuration changes in FLASH ROM (permanent memory). The changes are lost if not saved to FLASH ROM or if power is lost before you can save them.
- Commands to **delete** a network user, interface, route, TCP connection, community name, network service and others cannot take place unless the process or function has first been disabled.
- Wherever an **IP address** value is required, you can enter a host **name** provided you have configured a DNS server or put the name and address into the DNS Local Host table.
- Elements like vc's and users must be **disabled** before changes to these elements can be implemented.

Command Language Terminology

The CLI command language creates, manages, displays and removes system entities. These entities describe system and network connections and processes. Most of the managed entities in the system are slotted in tables. Some common examples are:

- **Network** - defines local and remote networks, network connections, hosts and routers
- **VC** - A table of parameters that describes connection parameters associated with a remote site. These parameters are used when establishing a network connection over the WAN.
- **User** - A table of parameters that describes connection parameters associated with Telnet users that wish to attach and remotely manage the unit.
- **Filter** - can be applied to interfaces, connections, and users to control access through the system
- **Interface** - describes physical devices; for example, ports
- **Syslog Host** - receives system messages
- **DNS Server** - translates IP addresses to and from host names
- **Route** - describes a path through the network to another system or network

Table entries are created with an **add** command, and removed with a **delete** command. The **add** command specifies the most important parameters of the entry. Additional parameters are usually specified with the **set** command, which is also used to change configured parameters.

The **list** command displays table entries. For example, **list users** displays all defined administrative login profiles. The **show** command displays detailed information about a specific table entry. For example, **show user root** displays detailed information for the administrative login profile *root*.

3 CONFIGURATION METHODS

The OCR 812 CLI offers three setup choices, all of which are described in this section: the automated, *Quick Setup* method, the *QuickVC Setup* method, and the *manual* method. Review the capabilities of each below and decide which configuration method best suits your needs, then proceed to the appropriate chapter for detailed configuration guidelines for each method.

Quick Setup Instructions

The *Quick Setup* program for the CLI is designed to get your OCR 812 up and running fast. To ensure that you have all the information you need on hand *before* you engage Quick Setup, we have supplied a script to jot down system, management, and LAN configuration information. We recommend that you fill out either script completely to get the full benefit of the program.

Used in combination with the QuickVC Setup program, Quick Setup allows virtually complete console-based configuration of your OCR 812 without requiring any knowledge of CLI command syntax.

The questions beginning in the next chapter represent nearly the full text of what Quick Setup would query if you were to use every service available as configured on the CLI. If you are using partial service - just IP configuration, for example - Quick Setup will skip the Bridging section. Default values are enclosed in brackets **[ ]**.

If at any time you decide to quit Quick Setup, you can type ***<ctrl>c (^c)*** *throughout the program.*

QuickVC Setup Instructions

The *QuickVC Setup* program for the CLI is designed to get virtual circuits for your OCR 812 configured quickly. To ensure that you have all the information you need on hand *before* you engage QuickVC Setup, we have supplied a script to jot down information for VC connections. We recommend that you fill out either script completely to get the full benefit of the program.

Used in combination with the Quick Setup program, QuickVC Setup allows virtually complete console-based configuration of your OCR 812 without requiring any knowledge of CLI command syntax.

The questions beginning in Chapter 5 represent nearly the full text of what QuickVC Setup would query if you were to use every service available as configured on the CLI. If you are using partial service QuickVC Setup will skip some sections. Default values are enclosed in brackets **[ ]**.

Manual Setup Instructions

Once you become familiar with the CLI interface, you might find it more efficient to manage the OCR 812 manually. Manual configuration is most versatile in that you only enter commands that need to effectively change from the current configuration. Also, many of the advanced features can only be accessed through manual configuration (such as filtering).

4

QUICK SETUP

This chapter will describe in detail the operations of the Quick Setup program. It will identify the required information, steps involved, and sample output scripts from the execution of this program.

CLI Quick Setup Script

Introduction

The CLI Quick Setup program allows you to quickly configure LAN-side, global and management settings for your OCR 812. Instead of using CLI commands, you will simply respond to a series of questions regarding different aspects of your configuration. The program will convert your responses into the appropriate CLI commands and execute them.

The CLI Quick Setup program automatically executes when the OCR 812 is powered on with no configuration and all DIP switches in the back of the unit are in the OFF position. This boot mode (the default) is called Unconfigured Mode.

Restoring the OfficeConnect Remote 812 to an Unconfigured State

An OCR 812 unit can be restored to an unconfigured state by ensuring all DIP switches are in the OFF position and then deleting the configuration using any of the following methods:

- Press the Configuration reset button on the back of the unit while powering on.
- Issue the **delete configuration** command from the CLI***.***
- Use the browser-based OfficeConnect Remote 812 Manager to delete the configuration.

For more information on OCR 812 boot modes see the OfficeConnect Remote 812 ADSL Router Installation Guide.

Booting an OfficeConnect Remote 812 in the Unconfigured State

When booting an OCR 812 in the unconfigured state, the 812 link to the DSLAM will not come up until you do ***either*** of the following:

- Abort Quick Setup.
- Continue answering the Quick Setup prompts.

This applies to the first-ever boot, and when you reboot after deleting the existing configuration. If you wait for the DSLAM link to come up (without aborting or continuing to answer the prompts), the 812 will ***not*** initiate DSLAM negotiation.

Downgrading the Remote 812 Software to a Previous Version

Downgrading the 812 software to an older version is ***not*** recommended (we suggest you *upgrade* to obtain the latest and most reliable software available). If you do choose to downgrade, we suggest you delete your existing configuration before or after you install the downgrade (in any case, you must delete the existing configuration).

Installation of a downgraded version of the Remote 812 software (a version older than the version currently installed) is likely to cause a reduction in functionality. The reduction in functionality you experience may be substantial or minor, depending on which version you have before the downgrade, and which version you downgrade to.

Quick Setup Script Instructions

The following sections contain the CLI Quick Setup script. You will be required to enter information concerning your network configuration. Questions in the script are presented here in tables. Write the appropriate information for your desired configuration in the tables appearing throughout this section.

Quick Setup (CLI) is designed ***only*** *for initial set up of the OCR 812. When setup is complete, this one-time program will alter your configuration files (which the program cannot edit). If you make an error and need to restart, use the* ***delete configuration*** *command to reboot and return to factory default settings.*

Quick Setup Script

The OCR 812 Quick Setup will let you set up LAN-side and global configuration for your system.To configure wide-area profiles you should run the OCR 812 VC Wizard using the QUICKVC command.

Do you want to continue Quick Setup?

The OCR 812 Quick Setup allows you to set up a simple configuration for IP, IPX, and bridging.

Please answer the questions presented below with "yes" or "no" to indicate which portions of the system you want to configure.

When Quick Setup displays a question it will display a default answer in square brackets, like "[yes]". If you simply press enter, this is the answer that will be used for you.

Password Protection

Question	Default	Your System
Do you want the CLI to be password protected?	[no]	
What is the console login password (no more than 8 characters)?	[ ]	

Which portions of the network do you want to configure?

Question	Default	Your System
Network management ?	[yes]	
IP ?	[yes]	

IPX ?	[no]	
Bridging ?	[no]	

Quick Setup Identification Information

Question	**Default**	**Your System**
Enter the name of your system:	[ ]	
Who is the system contact person?	[ ]	
Where is this system located?	[ ]	

Quick Setup Management Information

Question	**Default**	**Your System**
Do you want to be able to manage the system via SNMP?	[yes]	

An SNMP community names a group of systems that can manage your system via SNMP. It is a rudimentary form of security.

Question	**Default**	**Your System**
What SNMP community will manage this system?	[public]	

Along with a community name, you can limit access to a specific management station. "0.0.0.0" means any station.

Question	**Default**	**Your System**
What is the IP address of the station for this community?	[0.0.0.0]	

You also need to specify if this community can only read information, or read and write information.

Question	**Default**	**Your System**
Can this community change management information?	[yes]	

This completes the section on SNMP management configuration.

TELNET information

Question	Default	Your System
Do you want to allow command line management via TELNET?	[yes]	

For TELNET management of the system, you need to create a user name and password to control access.

Question	Default	Your System
What user name will be allowed to manage this system?	[root]	
What password will be used for this user ?	[ ]	

Quick Setup IP Information

The OCR 812 uses a network name to identify the network for future management commands.

Question	Default	Your System
Enter the network name of your IP network:	[ip]	
Enter the IP address for the OfficeConnect Remote 812:	[192.168.200.254]	

The IP mask can be specified either as a class ("A", "B", or "C"), the number of one bits in the mask, or as an address in the format 255.x.x.x.

Question	Default	Your System
What should the mask be set to?	[C]	

You need to specify the framing for the IP network. It should be either "ethernet_ii" or "snap".

Question	Default	Your System
What is the framing for the IP network?	[ethernet_ii]	

You can use the Routing Information Protocol (RIP) to exchange routing information with other routers on the network.

Question	Default	Your System
Do you want to run RIP?	[yes]	
Choose the version of RIP to run:	[v2]	

The OCR 812 can act as a DHCP server, providing IP addresses to other stations on the local LAN.

Question	**Default**	**Your System**
Do you want the OfficeConnect Remote 812 to act as a DHCP server?	[yes]	
Enter the start address for the DHCP IP address pool:	[ ]	
Enter the end address for the DHCP IP address pool:	[ ]	

It is possible to restrict access to the TFTP server to a specific system or a list of systems. Quick Setup will allow you to enter one system that is allowed or allow access to all systems.

Question	**Default**	**Your System**
Do you want to allow all systems to access the TFTP server?	[yes]	

IP setup is completed.

Quick Setup IPX Information

The network name is used by the OCR 812 to identify your IPX network.

Question	**Default**	**Your System**
Enter the name of your network:	[ipx]	

The network number is a non-zero hexadecimal number of up to 8 digits.

Question	**Default**	**System**
Enter the ipx network number:	[ ]	

You need to specify the framing for the IPX network. It should be one of the following: “ethernet_ii”, “snap”, “dsap”, “novell_8023.”

Question	Default	System
What is the framing for the IPX network ?	[ethernet_ii]	

Quick Setup Bridge Information

The network name is used by the OCR 812 to identify your bridging setup.

Question	**Default**	**Your System**
Enter the network name:	[bridge]	

The spanning tree algorithm is used to eliminate loops in a network that is linked together with bridges.

Question	**Default**	**System**
Do you want to run the spanning tree algorithm?	[no]	

Would you like to review your current settings before executing [yes]?

Sample Identification Information

This section contains a sample of possible settings.

Management Information:	
Console Login Required:	yes
Console Login Password:	password
SNMP Management:	
SNMP Community:	public
SNMP IP Address:	0.0.0.0
SNMP Read&Write:	yes
TELNET Management:	
TELNET User:	root
TELNET Password:	!root
IP Information:	
IP Network Name:	ip
IP Network Address:	192.168.200.254
IP Mask:	C
IP Frame Type:	ethernet_ii
IP RIP:	v2
DHCP Server:	Enabled
DHCP Pool Start IP Address:	192.168.200.1
DHCP Pool End IP Address:	192.168.200.40
TFTP Server Information:	
TFTP Access:	Any system
IPX Information:	
IPX Network Name:	ipx
IPX Network Number:	12345661
IPX Frame Type:	ethernet_ii
Bridge Information:	
Bridge Network Name:	bridge
Spanning Tree:	no

Do you want to change any answers [no]?

Do you want to actually execute these commands [yes]?

Sample Output Display as Quick Setup Executes

```
OCR-DSL> set system name "name"
OCR-DSL>set system location "vienna"
OCR-DSL>set system contact "jc"
OCR-DSL>enable command password “password”
OCR-DSL>add snmp community public address 0.0.0.0 access RW
OCR-DSL>enable security_option remote_user administration
OCR-DSL>add user "root" password "!root"
OCR-DSL>add ip network “test” interface eth:1 address 192.168.200.254/C
frame ethernet_ii enable no
OCR-DSL>set dhcp mode server
OCR-DSL>set dhcp server start 192.168.200.1 end 192.168.200.40 router
192.168.200.254 dnsl 192.168.200.254 dns2 0.0.0.0 wins1 0.0.0. wins2 0.0.0.0
mask 255.255.255.0
OCR-DSL>add dns host ocrdsl-3com.com addr 192.168.200.254
OCR-DSL>enable dns
OCR-DSL>add tftp client 0.0.0.0
OCR-DSL>set ip network “test” routing ripv2
OCR-DSL>enable ip network “test”
OCR-DSL>enable ip forwarding
OCR-DSL>add ipx network “ipx” address 12345661 interface eth:1 frame
“ethernet_ii”
OCR-DSL>disable bridge spanning_tree
OCR-DSL>add bridge network “bridge”
OCR-DSL>save all
Saving..... SAVE ALL
SAVE ALL  Complete
OCR-DSL>Spawned Process CFP 282002 /./QuickSetup.commands Completed
Successfully
```

*Quick Setup (CLI) is designed **only** for initial set up of the OCR 812. When setup is complete, this one-time program will alter your configuration files (which the program cannot edit). If you make an error and need to restart, use the **delete configuration** command to reboot and return to factory default settings.*

5 QUICKVC SETUP

This chapter will describe in detail the operations of the OCR 812 QuickVC Setup Wizard program. It will identify the required information, steps involved, and sample output scripts from the execution of this program.

CLI QuickVC Setup Script

Introduction

The CLI QuickVC Setup program allows you to quickly configure remote site profiles (virtual channel connections) for your OCR 812. Instead of using cryptic commands you will simply respond to a series of questions regarding different aspects of your configuration. The program will convert your responses into the appropriate CLI commands and execute them.

The OCR 812 can be configured as an ATM device. Depending on the present configuration, the QuickVC script will prompt you for the appropriate parameters.

Instructions

This section contains the CLI QuickVC Setup script for all possible OCR 812 Virtual Channel (VC*)* configurations. You will be required to enter information concerning network configurations. Questions in the CLI QuickVC Setup script are presented here in tables.

Write the appropriate information for your desired configuration in the following tables.

Starting QuickVC Setup

```
OCR-DSL> quickvc
```

Welcome to the OCR 812 QuickVC Setup Wizard

The VC Setup Wizard allows you to add and configure a VC profile on your OCR 812. Each profile must have a unique name.

Question	Default	Your System
What is the name to be added ?	[ ]	

ATM Parameters

The characteristics of the ATM Virtual Circuit must be configured.

Question	Default	Your System
Enter the Virtual Path Identifier	[0]	
Enter the Virtual Channel Identifier	[0]	
Is the Category of Service (U)br or (C)br ?	[U]	
Enter the Peak Cell Rate:	[0]	

The Category of Service and cell rate parameters only affect data transmitted from the OCR 812 to the remote site (upstream direction). The default value of UBR with a Peak Cell Rate of 0 will attempt to use all available upstream bandwidth when transmitting to the remote site.

The ATM Configuration for VC “name” is now complete.

Network Service

The OCR 812 supports either PPP, PPPoE, or RFC 1483 encapsulation.

Question	Default	Your System
Select the encapsulation type	[ppp]	

PPP Parameters

(Only applicable if PPP or PPPoE is chosen as the network service.)

You must configure a name and password that will be used during the PPP authentication process.

Question	Default	Your System
What is the authentication name ?	[name]	
What is the authentication password ?	[ ]	

The authentication name for VC “name” is now complete.

IP Configuration (Network Service PPP)

(Only applicable if PPP or PPPoE is chosen as the network service.)

Port Address Translation (PAT) allows a single WAN-side IP address to be ‘shared’ by multiple LAN-side devices.

Local and remote IP addresses can be configured in two different ways, as follows:

- **Specified**: the IP address is always a specific address.
- **Learned**: the IP address is learned when the PPP connection is established.

One active VC profile can have its remote router installed as the default router in the OCR 812’s IP route table.

You can use Routing Information Protocol (RIP) to exchange routing information with other routers on the network.

Question	Default	Your System
Is IP traffic going to be routed over VC “name”?	[yes]	
Do you want to enable IP Port Address Translation (PAT)?	[yes]	
Is the remote IP address (S)pecified or (L)earned ?	[L]	
Enter the IP address of the router across the WAN: (specified only)	[ ]	
Enter the IP mask for the router across the WAN: (specified only)	[C]	
Is the local IP address (S)pecified or (L)earned ?	[L]	

Enter the local ip address for the WAN connection: (specified only)	[ ]	
Do you want to use “name”’s remote router as the default gateway ?	[no]	
Do you want to run RIP ?	[no]	
Enter the version of RIP to run: (if applicable)	[v2]	

The IP configuration for VC “name” is now complete.

IP Configuration (Network Service RFC 1483)

Port Address Translation (PAT) allows a single WAN-side IP address to be ‘shared’ by multiple LAN-side devices.

If you choose to run PAT the WAN interface must be Numbered. (i.e., there must be a local WAN-side IP address specified that must be on a different IP network than the LAN-side IP address). For a discussion of Numbered and Unnumbered interfaces, see “Configuring IP Routing” in the Online User’s Guide.

Local and remote IP addresses can be configured in two different ways:

- Specified: the IP address is always a specific address.
- Learned: the IP address can be learned using DHCP.

One active VC profile can have its remote router installed as the default router in the OCR 812’s IP route table.

You can use Routing Information Protocol (RIP) to exchange routing information with other routers on the network.

The IP mask can be specified either as a class (“A”, “B”, or “C”), the number of one bits in the mask, or as an address in the format 255.x.x.x.

Question	**Default**	**Your System**
Is IP traffic going to be routed over VC “name” ?	[yes]	
Do you want to enable IP Port Address Translation (PAT) ?	[yes]	
Are the IP addresses (S)pecified or (L)earned ?	[L]	
Enter the IP address of the router across the WAN:	[ ]	
Enter the IP mask for the router across the WAN:	[C]	
Is the WAN interface (U)nnumbered or (N)umbered ?	[N]	
Enter the local ip address for the WAN connection: (numbered only)	[ ]	
Do you want to use “name”’s remote router as the default gateway ?	[no]	
Do you want to run RIP ?	[no]	
Enter the version of RIP to run:	[v2]	

The IP configuration for VC “name” is now complete.

IPX Routing (Network Service PPP)

Question	Default	Your System
Is IPX traffic going to be routed over VC “name”?	[no]	
Is the IPX WAN interface (S)pecified or (L)earned?	[L]	
Is the IPX WAN interface (U)nnumbered or (N)umbered?	[N]	
Enter the IPX network number for the WAN?	[ ]	
Do you want IPX routing (RIP) to run over the WAN?	[yes]	

The IPX configuration for VC “name” is now complete.

IPX Routing (Network Service RFC 1483)

Question	Default	Your System
Is IPX traffic going to be routed over VC “name”?	[no]	
Is the IPX WAN interface (U)nnumbered or (N)umbered?	[N]	
Enter the IPX network number for the WAN?	[ ]	
Do you want IPX Routing (RIP) to run over the WAN?	[yes]	

The IPX configuration for VC “name” is now complete.

Bridging

Question	Default	Your System
Do you want to Bridge any traffic over VC “name”?	[no]	

The OCR 812 can be configured to send and receive the routed (IP and IPX) packets using bridged encapsulation (i.e., Bridged-1483 or BRCP or PP), where the MAC-header is included in each packet.

The routing rules for [IP and IPX] will be applied to each packet.

Question	Default	Your System
Do you want to enable MAC-encapsulated routing?	[no]	

Review

Question	Default	Your System
Would you like to review your answers before executing them?	[yes]	

Sample Identification Information

This section contains a sample of possible settings.

Encapsulation type:	PPP
ATM information:	
VPI/VCI:	0/33
Category of Service:	UBR
Peak Cell Rate:	0
IP:	Enabled
Local WAN IP Address:	Learned
Remote WAN IP Address:	Learned
WAN Interface Type:	Numbered
Address Translation (PAT):	Enabled
RIP:	no
Remote is Default Gateway:	yes
IPX:	Enabled
IPX WAN Network Number:	Learned
IPX WAN RIP:	Yes
Bridging:	Enabled

Question	Default	Your System
Do you want to change any answers?	[no]	
Do you want to actually execute these commands?	[yes]	

Sample Output Display as Quick Setup Executes

```
OCR-DSL> add vc “name”
OCR-DSL>set vc “name” ip disable ipx disable bridging disable
OCR-DSL>set vc “name” network_service ppp
OCR-DSL>set vc “name” atm vpi 0 vci 0 category_of_service unspecified pcr 0
OCR-DSL>set vc “name” ip enable
OCR-DSL>set vc “name” remote_ip_address 0.0.0.0/C
OCR-DSL>set vc “name” local_ip_address 0.0.0.0
OCR-DSL>set vc “name” ip_routing listen rip ripv2
OCR-DSL>set vc “name” nat_option enable
OCR-DSL>set vc "name" ipx enable
OCR-DSL>set vc "name" ipx_enable ipx_address 00000000 ipx_routing all
OCR-DSL>set vc “name” bridging enable
OCR-DSL>
OCR-DSL>enable vc “name”
OCR-DSL>_save users
_SAVE USERS Complete
OCR-DSL>Spawned Process CFP 272016 /./QuickSetup.commands Completed
Successfully
OCR-DSL>
```

6 MANUAL SETUP

This chapter describes how to manually set up the OCR 812 for routing *or* bridging.

Configuration Overview

The following steps provide an outline to follow when configuring the OCR 812 to route or bridge to remote networks.

1. Determine how the OCR 812 will be used (as an IP, IPX Router and/or Bridge) and gather information about your remote site connection using the Configuration Planning Forms provided with the unit.
2. Set up a remote site profile for each remote location including Network Service (PPP/PPPoE/PPPoA/RFC 1483), and WAN configuration.
   - Set up network (IP, IPX and/or Bridge) information:
   - Configure the network(s) over the LAN.
   - Add the network information to the remote site profile(s).
   - Turn RIP (IP and IPX) and SAP (IPX) on or off as needed for your configuration.
   - Add static and framed routes (IP and IPX) or services (IPX) if needed.
3. Optionally, set up DHCP and DNS information.
4. Optionally, perform system administration tasks such as setting the date and time, providing contact information, adding or changing Web browser or TELNET login access, and providing TFTP access.

You must assign a system name to the OCR 812 using the ***SET SYSTEM NAME <name>*** *command. If you do not assign a system name, the unit may reboot during PPP operation.*

5. Save the configuration.

The rest of this chapter provides an overview of OCR 812 basic operations and configuration, and is organized as follows:

- Remote Site Management
- IP Routing
- Address Translation
- DHCP
- DNS
- IPX Routing
- Bridging
- System Administration

Remote Site Management

Each remote site that you want to connect to is accessed through a single ATM Virtual Channel connection. To set up connections over the WAN, a VC (remote site) profile must be created and edited. With this profile, you specify ATM Virtual Channel information, protocols, and addresses that determine the method of connection and communication to that remote site.

You create VC profiles using the *add vc* command (e.g., **add vc Internet** will create a profile called “Internet”), and then you modify the profile using *set vc* commands to setup the WAN connection and network information.

The following list summarizes the necessary information.

- **WAN** - Network Service (PPP/RFC 1483) information, ATM VC information
- **IP** - IP addresses, address translation tables, static routes, RIP usage.
- **IPX** - IPX network address information, static routes and services, RIP usage.
- **Bridging** - Enable or disable bridging to the remote site.

If you need to connect to multiple remote sites (i.e., the Internet and a remote office) you should set up a remote site profile for each location.

*Remember to save your configuration using the **save all** command before rebooting your OCR 812 so that your changes will be written to permanent FLASH memory.*

Managing a Remote Site

- You can obtain a list of all currently configured VC profiles using the command:

  list vcs
- You can view the contents of a particular profile using the command:

  show vc <vc name>

The OCR 812 always has a *default* profile. Any value that is not set in a profile that you create will assume the values that are present in the *default* profile. The *default* profile cannot be created or deleted, but it can be modified using the **set vc** command.

- You can view the *default* profile using the command:

  show vc default

VC profiles can be enabled or disabled. When a profile is enabled using the *enable vc* command, the OCR 812 reads the connection parameters for the remote site from the profile and continuously attempts to establish a connection to the remote site.

When a profile is disabled using the *disable vc* command, the connection will be terminated and no other data will be directed to the remote site. Configuration changes to a remote site profile do not take effect until the next time the profile is enabled. Thus, if you want to make changes to the profile you should disable the profile, make your changes, and then re-enable the profile.

- For example, if you want to change the PPP authentication password to *testpassword* for a profile called *Internet* you would do the following:

  ```
  disable vc Internet
  set vc Internet send_password testpassword
  enable vc Internet
  ```

Configuring Network Service Information

A Network Service defines the data encapsulation and protocol characteristics for the connection between the OCR 812 and the remote site. The OCR 812 supports **four** types of Network Services: PPP, PPPoE, PPPoA, and RFC 1483. The OCR 812 and the remote site must both use the same Network Service in order for a connection to established and maintained.

Built-in client support for PPPoE and PPPoA in the OCR 812 enables users to take advantage of PPPoE and PPPoA authentication (both of which are widely used by Internet Service Providers) without having to make complex software changes to their PCs.

For PPP, PPPoE**,** and PPPoA network services, an authentication name and a password must be provided to establish the connection (note that the OCR 812 supports CHAP, MSCHAPv1, MSCHAPv2, and PAP authentication).

MPPE (Microsoft Point-to-Point Encryption) does ***not*** *support MSCHAPv****2*** *authentication. To use MPPE, you must set your system to use MSCHAPv****1****. If you want to use MPPE but cannot select MSCHAPv1, we suggest you set encryption to* ***NONE*** *(otherwise, it may be impossible to connect to sites that require some type of encryption).*

- To set up a profile for PPP, use the following commands:

  ```
  set vc <vc name> network_service ppp
  set vc <vc name> send_name <authentication name >
  set vc <vc name> send_password <authentication password>
  ```

- To set up a profile for PPPoE, use the following commands

  ```
  set vc <vc name> network_service pppoe
  set vc <vc name> send_name <authentication name >
  set vc <vc name> send_password <authentication password>
  ```

- To set up a profile for PPPoA, use the following commands:

  ```
  set vc <vc name> network_service pppoa
  set vc <vc name> send_name <authentication name >
  set vc <vc name> send_password <authentication password>
  ```

- To set up a profile for RFC 1483 (which does not support authentication), configure the Network Service using the command:

  ```
  set vc <vc name> network_service rfc_1483
  ```

When the Network Service is set to RFC 1483, the profile’s IP WAN addresses can be dynamically learned with the DHCP protocol. To enable DHCP on a Remote Site profile:

1 Set the network service to RFC 1483:

   set vc <vc name> **dynamic_ip_addressing dhcp_client**

2 Enable MAC encapsulated routing (MER):

   set vc <vc name> **mac_routing enable**

3 Set dynamic IP addressing to DHCP:

   set vc <vc name> **dynamic_ip_addr dhcp_client**

Enabling a Point-to-Point Protocol

PPP is enabled by default.

- To **enable** PPPoE (Point-to-Point Protocol over Ethernet) on a Remote Site profile, configure the Network Service using the command:

  set vc <vc name> **network_service pppoe**

- To **enable** PPPoA (Point-to-Point Protocol over ATM) on a Remote Site profile, configure the Network Service using the command:

  set vc <vc name> **network_service pppoa**

Configuring ATM Information

The ATM parameters are supplied by your service provider. These parameters consist of:

- ATM VC information
- ATM Category of Service parameters

ATM allows for permanent connections (PVCs) and switched connections (SVCs). For a PVC, the required VC information parameters consist of the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).

The VPI/VCI uniquely specify the path to the remote site and are placed in the ATM cell header that is used to route each cell to the remote site.

Two VC profiles with the same VPI and VCI cannot be enabled simultaneously. You may encounter this situation if you want to login to the same remote site with different PPP authentication parameters. You should delete all profiles using the same VPI/VCI and then enable the one that should be active.

Currently, the SVC capability is disabled in the OCR 812.

ATM Category of Service parameters specify characteristics (sometimes called traffic shaping parameters) for data transmitted from the OCR 812 to the remote site. They have no effect on data transmitted from the remote site to the OCR 812.

The ATM VC information and Category of Service parameters are entered into the profile using the ***set vc <vc name> atm*** command.

For PVCs, you must enter VPI and VCI information for each profile:

set vc name <vc name> **atm vci** <vci value> **vpi** <vpi value>

You should have been provided with Category Of Service parameters.

- UBR - Unspecified Bit Rate; No limit has been specified for the upstream data flow.
- CBR - Constant Bit Rate; A constant rate has been specified for the upstream data flow.
- The cell rate transmission parameters are used to specify upstream transmission rates for the particular Category of Service.
- PCR - the Peak Cell Rate is the maximum number of cells/second transmitted over this connection. The Peak Cell Rate is optional for UBR and required for CBR.
- To configure the profile for UBR, use:

  set vc <vc name> **atm category_of_service unspecifed pcr** <cell rate >
- To configure the profile for CBR:

  set vc <vc name> **atm category_of_service constant pcr** < cell rate >

  where the **pcr** parameter is used for the constant bit rate that is desired instead of as the peak cell rate.

If no traffic shaping parameters have been provided you should choose UBR with a PCR value of 0. The OCR 812 will attempt to use all of the upstream bandwidth when transmitting data to the remote site.

Setting Up a Virtual Private Network (VPN) Tunnel

You can create a VPN tunnel for two nodes connected through an 812 ADSL Router. OCR 812 support of the following protocols makes it possible for you to establish a VPN tunnel between OCR 812 and a remote private LAN:

- PPTP (Point-to-Point Tunnelling Protocol)

  PPTP is the defacto (unofficial) standard VPN tunnelling protocol.
- L2TP (Layer 2 Tunnelling Protocol)

  An extension to PPP (Point-to-Point Protocol), L2TP merges the best features of PPTP (from Microsoft) and L2F (from Cisco Systems). Like PPTP, L2TP requires that the Internet Service Provider's routers support it.

Tunnel Encryption

The OCR 812 can use Microsoft Point-to-Point Encryption (MPPE) to encrypt data transported over PPTP VPN connections. In any case, we suggest you set up **some** form of encryption for your tunnels.

To learn how to use the CLI to set up encryption on the OCR 812, please refer to the following sections:

- Encrypting a PPTP or L2TP Tunnel
- Configuring Windows 2000 Server to Support Encryption for L2TP Tunnels
- Configuring a Cisco Router to Support Encryption for L2TP Tunnels

VPN Tunneling Overview

A *VPN tunnel* is a private virtual circuit that uses public wires to connect two nodes. For example, it is common practice to create VPNs that use the Internet as the *public* medium over which *private* information is sent and received.

Tunnelling is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating a network protocol within packets carried by the second network. Using this technology, you can transport data over the Internet between administrative domains that use a protocol the Internet does ***not*** support (specifically, this is done by embedding private data inside TCP/IP packets).

On the 812 ADSL Router, tunnelling is accomplished by encapsulating protocol A within protocol B. In effect, protocol A treats protocol B as if B were the Data Link layer (the OSI layer concerned with physically passing data from one node to another).

Before You Begin

Before you can initiate a VPN tunnel to a remote private network, you (or a network administrator) must do all of the following:

- **On the Remote Private Network ("Server") Side:**
  - Set up a PPTP tunnel server (also called a tunnel "terminator") on the remote private network.

    Examples of a PPTP tunnel server are a Windows NT server (Windows 2000, version 4.0 or later, with Service Pack 3 or greater and RAS installed) or 3Com's Total Control Hub.
  - Install any networking protocols required for the private network on the PPTP tunnel server (such as IP, IPX, and NetBeui).
- **On the 812 ADSL Router ("Client") Side:**
  - Configure the OCR 812 for a VPN.
  - Install any networking protocols required for the private network on each *workstation* that will establish a VPN tunnel.

Initiating a VPN Tunnel

Any user on a local private LAN can send traffic to a user on a remote private LAN. When a user on the local LAN sends a packet to a user on the remote LAN, the OCR 812 detects this attempt and automatically places a call to the remote LAN. Once the call is connected, a VPN tunnel is automatically initiated (created ***and*** enabled) between the OCR 812 and the tunnel server at the remote private network.

A VPN tunnel gives you access to a remote private LAN without requiring you to implement a direct physical connection. In addition, once your ISP connection is established, other users on the same local and remote LANs can use the existing VPN tunnel.

The default setting for VPN tunnels is **disabled**.

Enabling and Disabling a VPN Tunnel

To enable a VPN, enter the **enable tunnel** command. To disable a VPN, enter the **disable tunnel** command.

Before you attempt to set or change any parameter for a VC, you must first disable the VC using the ***DISABLE VC <vc_name>*** *command. If you attempt to set or change VC values while the VC is enabled, an* ***erroneous*** *error message (telling you that you must first disable the VC) will display. Whether you disable first or not, the change* ***will*** *take effect.*

Before you attempt to set or change tunnel parameters via the OCR 812 web configurator, you must first disable the tunnel using the ***DISABLE TUNNEL <tunnel_name>*** *command (if you do not follow this procedure, your changes will* ***not*** *take effect, and no error message will display). You do not need to disable a tunnel before making changes via the CLI, but it is recommended that you do so as a matter of good practice.*

Displaying VPN Tunnel Information

You can display a list of the tunnels created on the OCR 812, and their status (active or inactive) by entering the **list tunnels** command.

To check the parameters of a tunnel, enter the **show tunnel** command. To delete a tunnel, enter the **delete tunnel** command.

Creating a VPN Tunnel Using 812 Default Values

To add a VPN tunnel using 812 default values, enter the **add tunnel** command. 812 VPN tunnel default values are shown in Table 6-1.

Table 6-1 Default Tunnel Values (812 ADSL Router)

Parameter	Default Value	Remarks
STATUS	DISABLED	
INPUT_FILTER	no filter	
OUTPUT_FILTER	no filter	
PASSWORD	“ ”	***(See Notes below)***
SEND_PASSWORD	“ ”	By default, is a duplicate of the PASSWORD. See note below.
ENCRYPTION_ALGORITHM	NONE	
MTU	1400	
TUNNEL_TYPE	PPTP	
SEND_NAME	*tunnel_name*	Any name you give the tunnel in the **ADD TUNNEL** command will be duplicated in the SEND_NAME by default.
NAT_OPTION	PAT	
LOCAL_IP_ADDRESS	255.255.255.255	

When adding a TUNNEL you cannot set the PASSWORD or SEND_PASSWORD in the ***ADD TUNNEL*** *command. The default PASSWORD and SEND_PASSWORD will* *be blank (assigned with the value ""). You can change the PASSWORD and SEND_PASSWORD using the SET TUNNEL [PASSWORD | SEND_PASSWORD] command. You **must** change the SEND_PASSWORD (to the appropriate authentication password value expected by the VPN Server) using the SET TUNNEL < tunnel_name> SEND_PASSWORD command. You may **optionally** change the PASSWORD using the SET TUNNEL < tunnel_name> PASSWORD command.*

ℹ *You must make sure that the tunnel is **disabled** before you attempt to change the passwords.*

Tunnel Commands

The commands presented in this section enable you to display tunnel information, enable and disable a tunnel, and set the tunnel parameters shown in Table 6-2.

add tunnel <tunnel_name>

Use this command to set up a VPN tunnel with the default values shown Table 6-1.

Optionally, specify the server end point and the remote ip address as follows:

```
SERVER_END_POINT <HOST_NAME OR IP_ADDR>
```

ℹ *A remote_ip_address value specified as an add tunnel command option should be 255.255.255.255 (this is the **default** value).*

delete tunnel <tunnel_name>

Use this command to delete the tunnel.

enable tunnel <tunnel_name>

Use this command to activate the tunnel.

disable tunnel <tunnel_name>

Use this command to deactivate the tunnel.

list tunnel

Use this command to list the name and status of tunnels.

show tunnel <tunnel_name>

Use this command to display the parameter values currently defined for the specified tunnel.

set tunnel <tunnel_name>

Use this command to modify any of the parameters of the tunnel. The following is a list of **set tunnel** parameters and supported values:

Table 6-2 812 Set Tunnel Parameters and Supported Values

Parameter	Supported Value	Remarks
ENCRYPTION_ALGORITHM	NONE AUTO MICROSOFT_128BIT MICROSOFT_40BIT MICROSOFT_56BIT REQUIRED	
MTU	1400	
TUNNEL_TYPE	PPTP, L2TP	

Table 6-2 812 Set Tunnel Parameters and Supported Values

Parameter	Supported Value	Remarks
INPUT_FILTER	<filter_name>	
OUTPUT_FILTER	<filter_name>	
PASSWORD	<password>	
SEND_PASSWORD	<password>	The SEND_PASSWORD must match the authentication password on the VPN server. You must change the default SEND_PASSWORD using the **SET TUNNEL** command.
MTU	1400	
SEND_NAME	<name>	The SEND_NAME must correspond with the authentication name on the VPN server.
NAT_OPTION	PAT	
LOCAL_IP_ADDRESS	<ip_address>	255.255.255.255 is the recommended setting for LOCAL_IP_ADDRESS
REMOTE_IP_ADDRESS	<ip_address>	255.255.255.255 is the recommended setting for REMOTE_IP_ADDRESS

For example, to change the SEND_PASSWORD settings of a tunnel named ZOOM to VPN, enter the following command:

```
SET TUNNEL ZOOM SEND_PASSWORD VPN
```

*You must disable the tunnel using the **disable tunnel <tunnel_name>** command before you can change any parameters.*

Creating a VPN Tunnel Using Non-Default Values

To change any of the default values for a VPN tunnel created using the **add tunnel** command, enter the **set tunnel** command.

Encrypting a PPTP or L2TP Tunnel

Encryption protocols can be used in conjunction with authentication protocols to ensure that the VPN, private networks, and private data cannot be accessed or intercepted by unauthorized parties. To set up encryption for any VPN tunnel, you can use either the OCR 812 web configurator or the OCR 812 CLI.

- To learn how to set up encryption using the CLI, see Configuring Authentication and Encryption.
- To learn how to set up encryption using the OCR 812 web configurator, see the *Online User's Guide*, the section called “Configuring Virtual Private Networks”.

Configuring Authentication and Encryption

To learn how to use CLI commands to configure authentication and encryption for the OCR 812, please refer to the following:

- To configure authentication parameters, see set ppp receive_authentication [ANY | ANY_EXCEPT_MSCHAP | CHAP | MSCHAPV1 | MSCHAPV2 | NONE | PAP].
- To configure a Windows 2000 Server for CHAP authentication, see Configuring Windows 2000 Server to Support CHAP Authentication.
- To configure MPPE encryption, see set tunnel <tunnel_ name>encryption_algorithm [AUTO | MICROSOFT_128BIT | MICROSOFT_40BIT | MICROSOFT_56BIT | NONE | REQUIRED].
    - To set up MPPE, note that you must **also** configure the OCR 812 to use the MSCHAPv1 authentication protocol.

      To configure the OCR 812 to use MSCHAPv1, enter the set ppp receive_authentication [ANY | ANY_EXCEPT_MSCHAP | CHAP | MSCHAPV1 | MSCHAPV2 | NONE | PAP] command and specify the MSCHAPv1 option.
    - To learn more about MPPE, please visit the Microsoft corporate web site at www.microsoft.com.
- To configure a Windows 2000 Server for L2TP encryption, see Configuring Windows 2000 Server to Support Encryption for L2TP Tunnels.
- To configure a Cisco Router for L2TP encryption, see Configuring a Cisco Router to Support Encryption for L2TP Tunnels.

Configuring Windows 2000 Server to Support CHAP Authentication

Microsoft supports CHAP authentication for both PPTP and L2TP tunnels. However, to configure CHAP authentication for a Windows 2000 Server, you must ensure that **store pw using reversible encryption for all users in domain** is set to enabled ***before*** adding users.

*If you add users before you enable **store pw using reversible encryption for all users in domain**, you must enable the option and then re-enter the passwords for all users in the domain.*

To Configure authentication for your Windows 2000 Server.

1 Set up the Windows 2000 Server with IP address 123.45.67.89.

2 Add the authentication protocols you wish to use. See Authentication Options for more information.

To configure CHAP authentication for your Windows 2000 Server, set **store pw using reversible encryption for all users in domain** to enable, as follows:

a Select Programs->Administrative Tools->Local Security Policy.

b Select Security Settings\Account Policies\Password Policy.

3 When prompted, enter the password secret.

4 Add all users for the domain.

An administrator may also set up a Windows 2000 Server as a router with a private IP subnet set to 98.76.54.0/C. To add DHCP Services on the Windows 2000 Server, an administrator can use any IP addresses from 98.76.54.1 to 98.76.54.253 inclusive. IP addresses for workstations on the private LAN side of the Windows 200 Server will be in the 98.76.54.xx subnet.

Configuring Windows 2000 Server to Support Encryption for L2TP Tunnels

Microsoft supports encryption for both PPTP and L2TP tunnels. However, to configure encryption for an L2TP tunnel connecting an OCR 812 with a Windows 2000 Server, you must modify your Windows 2000 Server Registry settings.

To configure Windows 2000 Server Registry settings to support L2TP encryption, perform the following steps:

1. Start the Registry Editor (Run Regedt32.exe).
2. Locate the following Registry key:

   \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan \Parameters
3. On the Edit menu, select Add Value.
4. In the Add Value window, specify the following Registry Value Name, Data Type, and Value:

   Value Name: **ProhibitIpSec**

   Data Type: **REG_DWORD**

   Value: **1**
5. Exit from the Registry Editor.
6. Restart your computer (Registry changes will ***not*** take effect if you do not restart the computer).

Configuring a Cisco Router to Support Encryption for L2TP Tunnels

Cisco routers support encryption for both PPTP and L2TP tunnels. However, to configure encryption for an L2TP tunnel you must first modify the router's default configuration settings.

To configure Cisco router settings to support encryption for an L2TP tunnel, perform the following steps:

1. In Cisco router configuration mode, enter the following commands to configure tunnel authentication:

   ```
   aaa authentication login cisco local
   aaa authentication ppp default local
   aaa authorization network default local
   username <username> password <password>
   ```
2. In Cisco router configuration mode, enter the following commands to configure the router as an L2TP server:

```
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 25
terminate-from hostname OfficeConnect
local name c7200
no l2tp tunnel authentication
source-ip 192.180.3.2
```

3 In Cisco router configuration mode, enter the following commands to configure the private network (LAN) interface:

```
interface Ethernet1/2
ip address 192.168.200.1 255.255.255.0
no ip mroute-cache
```

4 Before establishing the L2TP tunnel, you must first establish an ATM link between the OCR 812 and the Cisco router. To establish an ATM link, install an ATM interface card in the router and configure the card using the commands specified in step b.

a To install an ATM interface card in your Cisco router, please refer to the instructions provided by your interface card manufacturer.

b To configure an installed ATM interface card, enter the following commands:

```
interface atm 2/0
atm scrambling cell-payload
atm framing cbitplcp
interface ATM2/0.13148 multipoint
ip address 192.180.3.1 255.255.255.0
ip mask-reply
ip rip send version 2
ip rip receive version 2
map-group cpmtn
atm pvc 648 13 148 aal5snap
map-list cpmtn
ip 192.172.18.2 atm-vc 618 broadcast
```

5 Once the L2TP tunnel has been established (and authentication has been successful), the following Virtual Template will assign an IP address for the defined L2TP pool:

```
interface Virtual-Template25
ip unnumbered ATM2/0.53103
ip mroute-cache
peer default ip address pool L2TP
```

```
ppp authentication pap
```

6 Ensure RIP and IP Pool configuration parameters are set to the following values:

RIP Configuration

```
router rip
ver 2
network 192.180.3.0
```

IP Pool for L2TP Tunnel

```
ip local pool L2TP 192.168.200.3 192.168.200.10
```

At this point, your L2TP tunnel should be fully operational and ready for use.

Debugging an L2TP Tunnel on a Cisco Router

If your L2TP tunnel has not been successfully established, or if it is not operating as expected, use the following debug commands to identify and correct the problem(s) you are experiencing:

Debug vpdn command:

Parameter	Used to Debug
error	VPDN Protocol errors
event	VPDN event
l2tp-sequencing	L2TP sequencing
l2x-data	L2F/L2TP data packets
l2x-errors	L2F/L2TP protocol errors
l2x-events	L2F/L2TP protocol events
l2x-packets	L2F/L2TP control packets

Debug ppp command:

Parameter	Used to Debug
authentication	CHAP and PAP authentication
bap	BAP protocol transactions
cbcp	Callback Control Protocol negotiation
compression	PPP compression
error	Protocol errors and error statistics
multilink	Multilink activity
negotiation	Protocol parameter negotiation
packet	Low-level PPP packet dump
tasks	PPP background tasks

To configure encryption parameters using the OCR 812 web configurator, see the *Online User's Guide*.

Adding a Framed Route for a VPN Tunnel

If you wish to set up a route to a network on the private (LAN) side of a remote site, use a framed route.

To add a framed route for a VPN tunnel, enter the **add framed_route vc** command or the **add framed_route tunnel** command at the CLI prompt. For more information, see add framed_route vc <name> and add framed_route tunnel <tunnel_name> in Appendix B.

In the following example, the **add framed_route tunnel** command is used to set up a framed route for a VPN tunnel called mtm.

```
add framed_route tunnel mtm gateway 0.0.0.0. ip_route 191.168.0.0/B metric 3
```

Note that you can delete a framed route you have added by entering the **delete framed_route** command and specifying the name of the framed route you wish to delete. For more information, see Configuring Static and Framed IP Routes and delete framed route vc.

Before adding a framed route for a VPN tunnel, ensure that the tunnel is disabled. Once the tunnel has been disabled, you can then add the framed route using the ***add framed_route*** *command.*

A *framed route* is much like a static route in that you manually configure the route. The difference is that a *static route* is defined for the LAN while a framed route is associated with a remote site connection. Also, while a static route is active when the LAN is connected, a framed route is active **only** when the connection to the associated remote site is active.

IP Routing

The OCR 812 can be configured as an IP Router to forward packets between the local LAN interface and one or more remote sites.

A forwarding table is maintained which specifies which interface to route an IP packet based on the destination IP address. Entries in the forwarding table are both static and dynamic. Static entries are based on the LAN’s and remote site's subnet addresses and user configured static routes. Dynamic entries are added when RIP is enabled and routes are learned from neighboring routers.

To configure IP routing, IP must be defined on both the LAN interface and one or more VC profiles. On the LAN, an IP network must exist with a specified IP address and subnet mask. In the VC profile, IP routing needs to be enabled, and the remote router address, a remote subnet mask and local WAN interface address need to be configured. The remote site address configuration can be learned dynamically when the connection is established if the Network Service is PPP, otherwise it has to be specified.

Remember to save your configuration using the ***save all*** *command before rebooting your OCR 812 so your changes will be written to permanent FLASH memory (i.e. permanently saved).*

Enabling IP Routing

When the OCR 812 is to be used for IP Routing, IP forwarding must be enabled. This is a global setting for the entire router.

- To enable IP routing, use the command:

  enable ip forwarding
- To disable IP routing, use the command:

  disable ip forwarding

IP Forwarding refers to the routing of IP packets from one interface to another. It does not affect communicating to the OCR 812 itself. Even when IP Forwarding is disabled, you can perform non-routing functions such as use a Web browser to manage the unit and use PING.

In addition to IP forwarding, there is a global RIP setting. If RIP is globally disabled, it is disabled for all LAN and WAN networks. If RIP is globally enabled, it can then be specifically enabled or disabled on the LAN IP networks and in each remote site's VC profile.

- To globally enable IP RIP, use the command:

  enable ip RIP
- To globally disable IP RIP, use the command:

  disable ip RIP
- To see the current IP Forwarding and RIP status, use the following commands:

  show ip settings

  show ip routing settings

Configuring an IP Network over the LAN

To configure IP over the LAN, you need to assign an IP network to the LAN port with the *add ip network* command. Each network has a *network name*. You will use the *network name* when entering commands related to the network.

The CIDR-supported *network address* includes a local station address and subnet mask using the format: *nnn.nnn.nnn.nnn/A B C* or *8-30*. The first 4 octets describe the IP address, followed by the subnet mask (contiguous) designator.

You can specify the subnet in one of two ways: a class or numerical designation. If you specify a Class C subnet mask, for instance, this command will generate a 255.255.255.0 subnet value for you. If you specify the number of bits (to be set to 1), the acceptable range is 8-30. The network address is invalid if the portion of the station address not covered by the mask is 0.

Defining a numerical subnet is useful when your value falls in between classes. You can also *omit* the mask altogether; it will automatically be calculated from the address.

- To add an IP network over the LAN, use the command:

```
add ip network <network name>
    address <ip address/mask>
    frame [ETHERNET_II | SNAP]
```

You can obtain a list of all configured networks using the command **list networks**. To only list IP networks, use **list ip networks**.

- By default, the network is enabled when it is created. You can disable the network using the following command:

  disable ip network <network name>
- You can delete a disabled network using the command:

  delete ip network <network name>

The *reconfigure ip network* command can be used to modify an existing IP network's address or frame type.

Configuring IP RIP on the LAN

IP RIP is configurable on each LAN IP network. The OCR 812 supports two versions of RIP, V1 or V2. You can also disable RIP completely.

- To set enable/disable RIP or set the version to use for a particular LAN IP network, use the command:

  set ip network <network name>
    routing_protocol [NONE | RIPV1 | RIPV2]

Other permutations of the *set ip network* command can be used to configure advanced RIP features and policies.

Configuring IP for the Remote Site Connection

In order to enable IP to be routed to a remote site, you must configure the following items in the VC profile associated with the remote site connection.

- You must enable IP routing in the profile
- You must enter the remote IP address information
- You must enter the local IP address information
- To enable or disable IP routing in a VC profile, use the command:

  set vc <vc name>
    ip [DISABLE | ENABLE]

The remote IP address information consists of the IP address of the router at the other end of the VC connection. This address can be either specified by you, or (if you are using PPP as the Network Service for the connection) it can be learned when the PPP session is established.

- To specify the remote IP address, use the command:

  set vc <vc name>
    remote_ip_address <ip address/mask>
- To specify that the remote IP address should be learned you can enter 255.255.255.255/H for the <ip address/mask> parameter, or you can use the command:

  set vc <vc name>
    address_selection negotiate

The IP address associated with the local side of the WAN connection can be specified by you, learned from the remote site (if you are using PPP as the Network Service for the connection), or the interface can be Unnumbered.

- To specify the local IP address use the command:

  set vc <vc name>
    local_ip_address <ip address>

To specify that the local IP address should be learned you must enter 255.255.255.255 for the <ip address> parameter. To specify that the interface is Unnumbered you must enter 0.0.0.0 for the <ip address> parameter.

For a discussion of Unnumbered (and Numbered) interfaces, see "Configuring IP Routing" in the *Online User's Guide*.

Optionally, you can specify that the remote site should be used as the default gateway.

- To designate the remote site as the default gateway use the command:

  set vc <vc name>
    default_route_option [DISABLE | ENABLE]

The default_route_option can only be enabled in one VC profile.

Also, you can configure IP Source Validation for the connection. When IP Source Validation is enabled, the source address of all IP frames received from the remote site will be validated. A packet's source address is valid if the OCR 812 will route an IP frame destined to the source address on the same VC it came in on.

- To enable IP Source Validation in a profile, use the command:

  set vc <vc name>
    ip_source_validation [DISABLE | ENABLE]

- To create a filter to block NetBIOS file and printer sharing over the Remote Site connection, use the following command:

  add auto_filter vc_blk_netbios vc <user name>

  Where <user name> is the VC Remote Site profile name.

This command creates a filter which rejects incoming frames with destination UDP ports 137 and 138, and destination TCP ports 139 and 143. The filter is automatically added to the filter manager and attached as the Remote Site's profile input filter.

Configuring IP RIP for a Remote Site

IP RIP can be enabled or disabled for each remote site connection.

The OCR 812 supports two versions of RIP, V1 or V2. Additionally, you can configure whether the OCR 812 should advertise local routes, only listen for routes from the remote site, or both.

- To configure RIP for a remote site connection:

  set vc <vc name>
    ip_routing [BOTH | LISTEN | NONE | SEND]

If you are using address translation for a remote site connection (NAT) you must set ip_routing to LISTEN or NONE. This is because you have set up a private LAN network and therefore do not want to be broadcasting information to other routers. The OCR 812 will not allow a profile using address translation to be enabled if ip_routing is set to BOTH or SEND.

- To configure the RIP version for the remote site connection use:

  set vc <vc name>
    rip [RIPV1 | RIPV2]

Configuring Static and Framed IP Routes

A *static route* is a configured route that will remain in the routing table until deleted. Static routes differ from *dynamic routes* in that dynamic routes are learned real-time via RIP.

A *framed route* is much like a static route in that you manually configure the route. The difference is that a static route is defined for the LAN while a framed route is associated with a remote site connection. Also, while a static route is active when the LAN is connected, a framed route is active **only** when the connection to the associated remote site is active.

If you wish to set up a route to a network on the other side of a remote site, use a framed route. If you wish to set up a route to a network through the LAN, use a static route. Only use static and framed routes for networks not learned using RIP.

- To add a static route over the LAN, use the command:

  add ip route <ip network address>
    gateway <ip address>
    metric <metric>

The route will appear in the IP routing table. You can display all IP routes with the **list ip routes** command.

- To delete an IP static route, use the command:

  delete ip route <ip network address>

- To add a framed route that will be installed in the IP routing table when a connection is established, use the command:

  add framed_route vc <vc name>
    ip_route <ip network address>
    metric <metric>

where *gateway* is the address of the remote router.

The route will be removed from the routing table when the VC profile is disabled.

- To delete a framed route so that it no longer will be installed in the routing table when the connection is established use the command:

  delete framed_route vc <vc name>
    ip_route <ip network address>

Remember to disable and then re-enable the VC profile for the change to take effect.

IP Tools

The OCR 812 CLI provides a standard set of IP utility programs including Ping, TELNET and RLOGIN.

Address Translation

Public IP addresses are registered and can be used within a public network (e.g., the Internet). Due to the limitation of IP version 4 address space and the growth of the Internet, public addresses are becoming more scarce. One solution to this problem is to use private addresses on small LANs and to use Address Translation when accessing devices on the public network. *Address Translation* changes an IP frame's *private* address to a *public* address at the gateway of a public network (i.e., the OCR 812).

- Under **PAT**, the router maintains a table of active port numbers in order to support simultaneous connections from different workstations on the LAN with ***one*** public IP address. This public address is the WAN interface address of the Remote Site profile. The WAN interface address can be statically configured *or* dynamically learned (PPP).
- Under **NAT**, the router maintains a table of active IP addresses in order to support simultaneous connections from different workstations on the LAN with ***one or more*** public IP addresses. For NAT, one or more public addresses are assigned to you by your service provider. The OCR 812 uses NAT to statically or dynamically assign public addresses to workstations on your private LAN. Please do ***not*** use the WAN IP address as one of your NAT public addresses.
- Under **Super NAT**, the router maintains a table of active IP addresses in order to support simultaneous connections from different workstations on the LAN with ***one or more*** public IP addresses. The OCR 812 uses NAT to statically or dynamically assign public addresses to workstations on your private LAN.

  Essentially, Super NAT is a combination of NAT and PAT. If NAT is configured, NAT is used first (address assignment is static and/or dynamic). If *additional* local workstations try to access the public network, PAT is then used. In this way, Super NAT ensures that local workstations can always access the public network.

NAT, PAT, or Super NAT ?

NAT, PAT, and Super NAT can each be used to ensure optimal address translation. Network conditions are the primary factor to be considered when determining which address translation method should be used.

To determine which form of address translation is best for you, please observe the following guidelines:

- **NAT** should be used when the ISP assigns ***multiple*** public IP addresses to the site. NAT is enabled by default, but the ***user*** can manually select and enable NAT using CLI commands.

  NAT allows the use of more IP clients than would be permitted if you were to dynamically and statically map private IP addresses to ***one*** public address. When NAT is enabled, a limited number of private clients may access the public network (the number of private clients is determined by the number of available public IP addresses.)
- **PAT** should be used when the ISP assigns ***one*** public IP address to the site. The ***user*** can manually select and enable PAT using CLI commands.

PAT allows multiple private IP addresses to use one public IP address by dynamically and statically mapping each private IP source address and private IP source port ***to*** one public IP source address and one public IP source port.

- **Super NAT** should be used to optimize address translation when the ISP assigns ***multiple*** public addresses to the site.

  When Super NAT is enabled, the ***system*** automatically switches between PAT and NAT as follows:

  - The OCR 812 utilizes NAT until all available public IP addresses have been used.
  - When all public IP addresses have been used under NAT, the system switches to PAT in order to allow ***additional*** stations to access the Internet ("additional" meaning "beyond those allowed by the public ports"). *PAT continues to run until a NAT port frees up.*

  For more information, see Super Network Address Translation (Super NAT).

set vc <vc name> nat_option

Use the **set vc** <vc name> **nat_option** command to set the NAT operating mode for a vc profile.

Options available for the **set vc** <vc name> **nat_option** command are as follows:

- NAT
- PAT
- Super_NAT
- Enable
- Disable

For a vc added using QuickVC, NAT is enabled by default.

Port Address Translation (PAT)

PAT uses the TCP and UDP port numbers to map ***multiple private*** port addressed LAN workstations (i.e. multiple users) to ***one public*** WAN port address.

Please note the following:

- *For normal applications such as Web browsing and FTP transfers, PAT can be configured by just enabling the feature.* When accesses are originated from the LAN (which uses private addresses), a mapping is established between the (LAN) source port number and the (LAN) source private address. When the response is received on the public addressed WAN destination port, the destination port is mapped back to the (LAN) private address.
- *Static PAT port mappings (**or** the PAT default address) **must** be configured when an application will initiate a TCP or UDP connection from the public network.* If a public accessible server resides on a privately addressed LAN, static ports can be defined for the applications they are running. For example, TCP port 80 (for a Web server) and TCP port 21 (for an FTP server) can be statically assigned. The PAT default address can be used ***with or instead of*** static port assignments, and is set to the private address of a workstation on the local LAN. If an incoming IP data packet is received on a WAN port and

there is no existing dynamic or static port mapping, the packet will be translated using the PAT default address.

Configuring PAT

Typically, PAT only needs to be enabled **or** disabled for a remote site connection.

- Use the following command to configure PAT in a vc profile:

  set vc <vc name> **nat_option pat**

As previously stated, it is sometimes necessary to configure the workstation default address. The workstation default address should be set to the private address of a workstation on the local LAN. If a data packet is received on the WAN port and a port mapping does not exist, the frame will be translated using the workstation default address.

- Use the following command to set this field:

  set vc <vc name> **pat_default_address** <ip address>

Static port configurations map a public port to a private IP address/port. Both TCP and UDP static ports can be defined. Remote sites can have multiple static ports defined. If static ports and the workstation default address are *both* defined, the static ports take precedence.

- Static ports are defined for TCP and UDP ports with the following commands:

```
add pat tcp vc <vc name>
  public_port <port>
  private_address <ip address>
  private_port <port>

add pat udp vc <vc name>
  public_port <port>
  private_address <ip address>
  private_port <port>
```

Typically the private and public port numbers are configured for the ***same*** *value (e.g., "21" for an FTP Server). However, you can map multiple* ***public*** *port numbers to the same* ***private*** *port number. For example, if you want to support a Web Server on the LAN* ***and*** *be able to manage your OCR 812 with the Web Browser, you would define* ***two static ports*** *for the Web Server (TCP port 80) as follows:*

- *To support a Web Server on the LAN, configure your LAN Server with public port 80, private port 80, and the private address of the LAN Server.*
- *To manage your OCR812 with the Web Browser, configure your OCR812 manager with public port 8080, private port 80 and the private address equal to the Ethernet (LAN) port IP address.*

To ***access*** *the OCR812 from a Web Browser, enter public Address:8080 at the prompt. Note that the value 8080 was chosen for example purposes only. You can enter* ***any*** *value within the port number range (i.e. 81).*

Remember to save your configuration using the ***save all*** *command before rebooting your OCR 812 so your changes will be written to permanent FLASH* *memory. If you do not enter the **save all** command before a reboot, unsaved changes made since the last save will be lost.*

Intelligent PAT

Enabled by default, Intelligent PAT provides a "best guess" as to ***where*** an incoming packet should be delivered *when*:

- A default PAT destination address has *not* been configured for a receiving (LAN) workstation

  -AND-

- Static TCP or UDP ports have not been configured

Intelligent PAT bases this "best guess" on an analysis of recent communication between the following:

- *This* remote workstation (the workstation sending this non-addressed packet from the WAN side of the OCR 812)
- Private workstations (on the LAN side of the OCR 812) that recently transmitted outgoing packets to *this* remote workstation

*Upon completion of the "best guess" analysis, Intelligent PAT forwards the packet to the **last** LAN workstation to transmit a packet to **this** remote workstation.*

Please also note the following:

- The “best guess” LAN workstation will continue to receive all non-addressed packets sent by *this* remote workstation until and unless a *new* (different) communication pattern is detected by Intelligent PAT.
- When a new communication pattern is detected, Intelligent PAT makes a new “best guess”, with the following results:
  - *Intelligent PAT begins to forward all non-addressed packets sent by the remote workstation to the newly chosen “best guess” LAN workstation.*
  - *The LAN workstation **previously** selected to receive all non-addressed packets from the remote workstation **no longer receives them**.*

Use the following command to configure Intelligent PAT:

set vc <vc name> **intelligent_pat_option** <Enable/Disable>

Monitoring PAT

The PAT configuration is displayed when viewing the remote site configuration using the *show vc* command. The *Network Address Translation* field should indicate “port (PAT)”. The *PAT Default Address* field will contain 0.0.0.0 if the option is ***disabled***, or a valid workstation IP address on the local LAN if it is ***enabled***. The static and/or dynamic address definitions are appended to the display only when configured.

- When the remote site is active, current **port** mappings and **address** mappings are displayed with the following commands, respectively:

  list nat vc <vc name> **port**

  list nat vc <vc name> **addr**

Network Address Translation (NAT)

NAT maps ***one private*** LAN IP address (one user) to ***one public*** (WAN) IP address. When using NAT, multiple users can access a single application at the same time.

Configuring NAT

When you create a vc using QuickVC, you are asked if you want to enable PAT. During QuickVC setup, you can:

- Accept the default choice (YES) to enable nat_option PAT.
- Choose *not* to enable PAT

If you simply use the add vc <vc name> command without specifying a NAT option, the default is NAT *disabled* (meaning that NAT, PAT, ***and*** Super NAT are ***not*** enabled).

Enabling NAT

To *enable* NAT, enter the following command:

set vc <vc name> **nat_option** nat

Configuring NAT Static and Dynamic Mappings

If you do not configure static or dynamic mappings for NAT (even if they have a default PAT address), the following error message displays on the CLI console when you enable the vc:

```
When Network Address Translation (NAT, RFC 1631) is enabled, Static Addresses and/or Dynamic
pool addresses must be configured.
```

- To configure *static* mappings for NAT, enter the following command:

  add nat static <vc name> **public_address** <ip address> **private_address** <ip address>

- To configure *dynamic* mappings for NAT, enter the following command:

  add nat dynamic <vc name> **public_address** <starting ip address> **count** <size of address pool>

Do not use the public WAN port IP address of the OfficeConnect 812 as one of the NAT static or dynamic public IP addresses.

Monitoring NAT

The NAT configuration is displayed when viewing the remote site configuration using the *show vc* command.

- The *Network Address Translation* field should indicate “RFC 1631 (NAT)”.
- The *NAT Default Address* field will contain the ***PAT*** default address if the option is ***disabled***, or a valid workstation IP address on the local LAN if it is ***enabled***.
- The static and/or dynamic address definitions are appended to the display only when configured.
- When the remote site is active, current port mappings and address mappings are displayed with the following commands, respectively:

  list nat vc <vc name> **port**

  list nat vc <vc name> **addr**

Super Network Address Translation (Super NAT)

Typically, the user must decide when to use NAT and when to use PAT, and switching between address translation modes must then be performed *manually* (by the user) as changing network conditions warrant. By contrast, with Super NAT enabled on the OCR 812, the ***system*** (not the user) ***automatically determines*** when it is best to use NAT, and conversely, when it is best to use PAT. Super NAT makes optimal use of available IP Addresses by enabling the system to automatically ***switch*** between PAT and NAT when multiple public addresses are assigned to the site.

Configuring Super NAT

You can configure NAT, PAT, or *both* NAT and PAT.

To use Super NAT, the system must first be configured to use both NAT and PAT, and Super NAT must *then* be enabled.

*The user is **not** required to add static or dynamic mappings for Super NAT. If no mappings are configured, the address translation mode will automatically be set to PAT.*

If you choose (optionally) to add static or dynamic mappings for Super NAT, do not use the public WAN port IP address of the OfficeConnect 812 as one of the Super NAT static or dynamic public IP addresses.

To configure OCR812 to use Super NAT, perform the following steps:

1. Configure all **NAT** and **PAT** parameters.

   a. To set up **NAT** parameters, enter the following CLI commands:

      add nat dynamic vc <vc name> **public_pool_start** <ip address> **count** <number>

      -AND / OR-

      add nat static vc <vc name> **public_address** <ip address> **private_address** <ip address>

   b. To set up **PAT** parameters, enter the following CLI commands:

      set vc <vc name> **intelligent_pat_option** *[enable/disable]*

      set vc <vc name> **pat_default_address** <ip address>

      add pat tcp vc <vc name> **public_port** <port> **private_address** <ip address> **private_port** <port>

      add pat udp vc <vc name> **public_port** <port> **private_address** <ip address> **private_port** <port>

2. To enable Super NAT, enter the following CLI command:

   set vc <vc name> **nat_option super_nat**

3. To display the ports or IP addresses being used by workstations on the remote connection, enter one of the following commands:

   a. To display ports:

      list nat vc <vc name> **port** <port>

   b. To display ip addresses:

      list nat vc <vc name> **addr** <ip address>

Monitoring Super NAT

The NAT configuration is displayed when viewing the remote site configuration using the *show vc* command. The *Network Address Translation* field should indicate "RFC 1631 (NAT)". The *NAT Default Address* field will contain the ***PAT*** default address if the option is ***disabled***, or a valid workstation IP address on the local LAN if it is ***enabled***. The static and/or dynamic address definitions are appended to the display only when configured.

- When the remote site is active, current port mappings and address mappings are displayed with the following commands, respectively:

  list nat vc <vc name> **port**

  list nat vc <vc name> **addr**

Configuring the 812 for SIP Phone Support

The OCR 812 can be configured to use SIP phones.

Overview

A SIP phone (Session Initiation Protocol phone) is a network-capable telephone that uses Ethernet connectivity to place and receive calls over the Internet. SIP phones send and receive voice data as TCP/IP packets. A SIP phone can be used for telephony, and to set up conferencing, multimedia, and other types of Internet communication sessions. SIP may also serve as the platform of choice for new types of communication like instant messaging, and it can be used to provide application-level mobility across networks (such as wireless).

Using a SIP Phone with the OfficeConnect Remote 812

To use a SIP phone with the OCR 812, your SIP phone must be installed on the LAN (private) side of the 812.

If you wish to use a SIP phone **and** address translation on your OCR 812, you must have PAT (Port Address Translation) enabled.

CLI commands are *not* required for SIP phone use. To use a SIP phone with the OCR 812, just connect the RJ-45 ports on your SIP phone to the RJ45 ports on the 812.

SIP Phone Infrastructure

Major components of the SIP phone network infrastructure are as follows:

- LAN

  On the LAN side of the OfficeConnect 812 are SIP phones and workstations, each having a *private* IP address visible *only* to devices on the LAN side of the 812 (i.e., “behind” the 812).

  The LAN connects to the LAN port of the 812 ADSL Router.

- OfficeConnect 812 ADSL Router

  The 812 ADSL Router functions as a bridge/router between LAN devices (connected to the LAN port) and all “outside” devices accessible via the Internet by means of the 812 WAN port connector.

- WAN

  The WAN port of the OfficeConnect 812 is a *public* IP address representing all of the *private* IP addresses on the LAN side of a SIP phone connection. “Outside” devices on the public side of the connection (the Internet side) can see the WAN port address, but they cannot see the private (LAN) port addresses it represents.

- Proxy Server

  The primary function of a proxy server in the SIP phone network infrastructure is to map the *IP address* of a SIP phone to a unique alphanumeric *user name* and *password,* and to store this information (collectively called a “caller identity”) in the proxy server data base.

  A proxy server automatically creates a caller identity for a SIP phone when the user plugs that phone into an Ethernet port.

  When a SIP phone caller places a call to another SIP phone user (by dialing their user name and password), the proxy server looks up the intended recipient’s caller identity (and finds, then connects to, the recipient's *IP address*). *The IP address of the intended recipient is their (SIP) phone number.*

By creating and storing a caller identity, a proxy server enables party A to call party B (and vice-versa), even if the recipient's IP address (SIP phone number) is not specifically known to the caller. Additionally, through the implementation of a user name and password scheme, the proxy server provides a simple yet effective security mechanism for SIP phone callers and call recipients alike.

When a SIP phone user places a call to a conventional telephone connected to the PSTN (Public Switched Telephone Network), the call is passed to the conventional telephone via a voice gateway.

- Voice Gateway

  As the last major link in the SIP phone network infrastructure, the voice gateway forwards the IP address (SIP phone number) received from the proxy server to the telephone company's Central Office (CO). Once received by the CO, the IP address is mapped to a conventional (non-SIP) phone number. From this point on, the phone call is processed through the telephone company network like any other non-SIP phone call originating from a conventional telephone.

For more information about 3Com SIP phone products, please see our web site at **`http://www.3com.com/products/sip`**.

DHCP

Dynamic Host Configuration Protocol (DHCP) is designed to provide a centralized approach for configuration of IP addresses and parameters.

When a workstation is configured for automatic assignment of IP addresses, it broadcasts a request out on the LAN. The DHCP Server responds with an IP address for the workstation, the domain name, and the IP addresses of the default router, two DNS Servers, and two WINS Servers.

The assignment of an IP address to the workstation is for a specified period of time, referred to as the lease period. Before the lease is set to expire, the workstation will send a request to the server to extend the lease period. The server maintains a list of assigned IP addresses and the duration period of the leases. When a lease expires, the IP address can be reassigned to another workstation.

The OCR 812 can be configured to support up to 40 workstations on the local LAN. In addition, the OCR 812 can be configured to be a DHCP Relay. When enabled, the Relay will process the broadcast request from the local workstation and send it to one or two remote DHCP servers. The response from the remote DHCP servers is processed and forwarded to the local workstation.

Remember to save your configuration using the ***save all*** *command before rebooting your OCR 812 so that your changes will be written to permanent FLASH memory.*

Configuring the DHCP Mode

The OCR 812 has three DHCP modes: Server, Relay and Disable.

- To configure the mode, use the following command:

  set dhcp mode [SERVER | RELAY | DISABLE]

Configuring the DHCP Server

The OCR 812's DHCP Server has the following fields that will need to be configured:

- Hostname
- Domain Name
- IP Address Pool, Start and End address
- IP Subnet address mask
- Lease period
- WINS Server addresses
- DNS Server addresses

The Hostname is the base name assigned to the workstation. A numeric suffix is appended to the base name and incremented after each assignment. For example, if the Hostname *unit* is configured, the first workstation will be assigned the Hostname *unit01*, the second workstation will be assigned *unit02* and so forth.

- Use the following commands to configure the DHCP Mode, base Hostname and the network's Domain Name:

  set dhcp mode server

  set dhcp server hostname <host name>

  set dhcp server domain <domain name>

The DHCP address pool is configured by specifying the starting and ending addresses of the pool. The range of the pool must be 40 addresses or less and must be entered on the same command line.

- The following set of commands configure the address pool and the network subnet IP address mask:

  set dhcp server start_address <ip address> **end_address** <ip address>

  set dhcp server mask <ip address>

- The final set of DHCP Server commands configure the Lease period and IP addresses of the Default gateway, WINS Servers, and DNS Servers. There can be up to two WINS and DNS Servers specified. If this functionality is to be disabled, an IP address of 0.0.0.0 is entered. If the OCR 812 is functioning as the DNS Proxy, the OCR 812's LAN IP address should be configured as the first (primary) DNS address.

  set dhcp server lease <seconds>

  set dhcp server router <ip address>

  set dhcp server wins1 <ip address> **wins2** <ip address>

  set dhcp server dns1 <ip address> **dns2** <ip address>

Monitoring the DHCP Server

There are monitoring commands which display the DHCP protocol counters and current lease information.

The DHCP protocol counters indicate the requests received, responses transmitted, and error indicators. The lease information indicates which IP addresses have been assigned, the corresponding workstation MAC addresses, and remaining time before the lease expires.

```
show dhcp server counters
list dhcp server leases
```

The DHCP Server configuration is displayed with the **show dhcp server settings** command.

Configuring the DHCP Relay

The OCR 812 can relay DHCP requests to up to two Remote Servers.

The OCR 812 DHCP relay can be configured with two Remote Server entries. Each entry consists of a server IP address, a specified maximum number of hops a request can take before being discarded, and enable flag.

- The following commands are used to configure the entries:

```
set dhcp mode relay
set dhcp relay server1 <ip address> max_hops <count> enabled [YES | NO]
set dhcp relay server2 <ip address> max_hops <count> enabled [YES | NO]
```

Monitoring the DHCP Relay

The DHCP relay has one command which displays the configuration and related counters. Counters include the number of requests transmitted and responses received from the remote servers.

- To show the configuration, use the command:

```
show dhcp relay
```

DNS

A *Domain Name Server* (DNS) provides an IP address for a host computer in a given Domain.

A *DNS Proxy* receives requests and attempts to find an entry in its local tables, and if one is not found, forwards the request to a remote server. The remote DNS Server can be learned dynamically through PPP or can be statically assigned.

The OCR 812's DNS Proxy enables you to configure remote DNS Servers for specific Domains. For instance, assume you have two remote sites configured, one to the Internet and the other to a corporate site which has a domain name of 3com.com. Two DNS remote servers can be configured, one which uses the corporate site for 3com.com and the other to use the Internet as the default.

The OCR 812's DNS Proxy also enables you to configure Static Host entries. The static table is checked first before the DNS request is forwarded on to the remote server. If the OCR 812 was first booted in DHCP Smart Mode, an entry, *ocrdsl-3com.com*, was automatically added to the table which maps to the OCR 812's local LAN IP address. This entry was added to simplify access to the OCR 812.

*Remember to save your configuration using the **save all** command before rebooting your OCR 812 so that your changes will be written to permanent FLASH memory.*

Configuring DNS

- To enable DNS functionality on the OCR 812, use the command:

  enable dns
- To disable DNS functionality, use the command:

  disable dns

You can configure three global DNS parameters that control the operation of the DNS proxy.

- *Number of Retries*: the number of retry attempts when accessing a primary or secondary DNS server. The default is 1 retry.
- *Timeout*: the amount of time to wait for request to be serviced. The default is 5 seconds.
- *Cache size*: the number resolved names to cache. The default is 100 entries.
- You can view the current DNS settings with the command:

show dns settings

- You can alter the current DNS settings with the command:

```
set dns
   cache_size <size>
   number_retries <number>
   timeout <seconds>
```

DNS Host Entries

- To add a DNS Host entry to the DNS Static Host table, use the command:

  add dns host <host name> **address** <ip address>
- To view the contents of the Static Host table, use the command:

  list dns hosts
- To delete a specific Host entry, use the command:

  delete dns host <host name>

Managing the DNS Proxy

When resolving a DNS name, the OCR 812 first searches for a match in the Static Host table. If a match is not found it will perform a proxy function. The DNS Server table contains a list of DNS Servers for specific domains. Each domain listed in the table can have up to two DNS Server addresses associated with it. The default domain has the name '*'.

Using PPP it is possible to learn DNS server addresses when the PPP session is established. In addition to specifying server addresses in the DNS Server table, you can specify a VC profile name that should be used to learn the addresses.

- To create a DNS Server entry when specific addresses are known, use the command:

  add dns server <domain name> **primary_address** <ip address> **secondary_address** <ip address>
- To create an entry that will learn addresses using PPP, use the command:

  add dns server <domain name> **vc** <vc name>

- To display the contents of the DNS Server table, use the command:

  list dns servers

- To delete a domain entry, use the command:

  delete dns server <domain name>

Access Lists

Access lists enable you to restrict which Remote Subnets are allowed to access the Management services of the OCR812.

- To add a remote subnet to the access list, use the following command:

  add access <ip subnet address>

- To remove a subnet from the access list:

  del access <ip subnet address>

- To display the access list:

  list access

In addition to adding subnets to the list, you can enable access to all hosts on the local LAN.

- To enable LAN access:

  enable lan access

- To enable the Access List functionality:

  enable access_list

- To disable the Access List functionality:

  disable access_list

- To show the status of the Access List functionality:

  show access

IPX Routing

The OCR 812 can be configured as an IPX router to forward IPX packets between the local LAN interface and one or more remote sites. A forwarding table is maintained which specifies which interface to route an IPX packet based on the destination IPX network number. Entries into the forwarding table are both static and dynamic. Static entries are based on the LAN's network number, the remote site WAN interface number, and user configured static routes. Dynamic entries are added when RIP is enabled and routes are learned from neighboring routers.

To configure IPX routing, IPX must be defined on both the LAN interface and one or more remote sites. On the LAN, an IPX network must exist with a specified IPX network number. On the remote sites, IPX forwarding needs to be enabled, and the WAN interface address need to be configured. The WAN interface can be Unnumbered (set to 0), Numbered, or dynamically learned if PPP is used.

*Remember to save your configuration using the **save all** command before rebooting your OCR 812 so that your changes will be written to permanent FLASH memory.*

Enabling IPX Routing

Unlike IP, there is no setting on the OCR 812 that enables or disables IPX routing functionality on a global basis.

Configuring IPX for the LAN

To configure IPX over the LAN you need to assign an IPX network to the LAN port with the *add ipx network* command. Each network has a *name*. You will use the *name* when entering commands related to the network.

```
add ipx network <network name>
  address <ipx network address>
  frame [DSAP | ETHERNET_II | NOVELL | SNAP]
```

You can obtain a list of all configured networks using the command **list networks**. To only list IPX networks, use **list ipx networks**.

- By default, the network is enabled when it is created. You can disable the network using the following command:

  disable ipx network <network name>

- You can delete a disabled network using the command:

  delete ipx network <network name>

Configuring IPX for Remote Site Connections

In order to enable IPX to be routed to a remote site, you must configure the following items in the VC profile associated with the remote site connection.

- You must enable IPX routing in the profile
- You must enter the WAN IPX network information
- To enable or disable IPX routing in a VC profile use the command:

```
set vc <vc name>
  ipx [DISABLE | ENABLE]
```

The WAN IPX network information consists of the IPX network address for the wide area connection. The IPX network address associated with the WAN connection can be specified by you, learned from the remote site (if you are using PPP as the Network Service for the connection), or the interface can be Unnumbered.

- To specify the WAN IPX address using up to 8 hexadecimal characters, use the command:

```
set vc <vc name>
  ipx_address <ipx network address>
```

- To specify that the WAN IPX network address should be learned via PPP you can enter FFFFFFFF for the <ipx network address> parameter:

```
set vc <vc name>
  ipx_address FFFFFFFF
```

- To specify that the interface is Unnumbered you must enter 00000000 for the <ipx network address> parameter.

  ```
  set vc <vc name>
   ipx_address 00000000
  ```

Configuring IPX Static and Framed Routes

A *static* route is a configured route that will remain in the routing table until deleted. Static routes differ from Dynamic routes in that Dynamic routes are learned real-time via RIP or when new connections are established.

A *framed* route is much like a static route in that you manually configure the route. The difference is that a static route is defined for the LAN while a framed route is associated with a remote site connection. Also, while a static route is active when the LAN is connected, a framed route is active **only** when the connection to the associated remote site is active.

If you wish to set up a route to a network on the other side of a remote site, use a framed route.

If you wish to set up a route to a network through the LAN, use a static route. Only use static and framed routes for networks not learned using RIP.

- To add a static IPX route over the LAN, use the command:

  ```
  add ipx route <ipx network address>
    gateway <ipx network address>
    metric <number>
    ticks <number>
  ```

The route will appear in the IPX routing table.

You can display all IPX routes with the **list ipx routes** command.

- To delete an IPX static route, use the command:

  ```
  delete ipx route <ipx network address>
  ```

- To add a framed route that will be installed in the IPX routing table when a connection is established use the following command:

  ```
  add ipx_route vc <vc name>
    ipx_net <ipx network address>
    metric <number>
    ticks <number>
  ```

The route will be removed from the IPX routing table when the VC profile is disabled.

- To delete a framed route so that it no longer will be installed in the routing table when the connection is established use the command:

  ```
  delete ipx_route vc <vc name>
    ipx_route <ipx network address
  ```

Remember to disable and then re-enable the VC profile for the change to take effect.

Configuring IPX Static and Framed Services

The Service table contains IPX server names, the *services* they provide, their network addresses and node addresses, and their relative distances. Examples of services include file servers and printers.

Note the following:

- A *static service* entry is a manually configured service accessible from the LAN. Once created, a static service entry remains in the Service table until deleted.
- *Static* services differ from *dynamic* services in that dynamic services are learned real-time via SAP packet exchange between routers.
- A *framed service* entry is a manually configured service accessible from the WAN. A framed service is active **only** when the connection to the associated remote site is active.

Use static and framed services for servers *not* learned using SAP.

- To add a static IPX service over the LAN, use the command:

  ```
  add ipx service <service name>
    gateway <network.node address>
    ipx_net <server network address>
    metric <number>
    node <server node address>
    socket <hex number>
    type <hex number>
  ```

The service will appear in the IPX Services table. For example:

```
add ipx service Serv411 gateway 98.0:0:0:0:0:0 ipx_net 31ab17c9
  metric 1 node 0:0:0:0:0:1 socket 451 type 4
```

You can display all IPX Services with the **list ipx services** command.

- To delete an static IPX service, use the command:

  ```
  delete ipx service <name> type <hex number>
  ```

- To add a framed service that will be installed in the IPX Services table when a connection is established, use the command:

  ```
  add ipx_service vc <vc name>
    hops <number>
    ipx_net <server network address>
    name <service name>
    node <server node address>
    socket <hex number>
    type <hex number>
  ```

The route will be removed from the IPX routing table when the VC profile is disabled.

- To delete a Framed route so that it no longer will be installed in the routing table when the connection is established use the command:

```
delete ipx_service vc <vc name>
   name <service name>
   type <type>
```

Remember to disable and then re-enable the VC profile for the change to take effect.

Configuring IPX RIP and SAP

IPX RIP is used to exchange IPX routing information with other IPX routers. SAP is a protocol used by IPX servers and routers to exchange information about the location of servers.

For IPX networks over the LAN you can separately enable or disable RIP and SAP. When enabled you can also specify whether RIPs or SAPs are sent, received, or both.

- To configure RIP for a LAN network, use the command:

  ```
  set ipx network <network name>
     rip [BOTH | DISABLE | LISTEN | RESPOND_ONLY | SEND]
  ```

- To configure SAP for a LAN network use the command:

  ```
  set ipx network <network name>
     sap [BOTH | DISABLE | LISTEN | RESPOND_ONLY | SEND]
  ```

Other permutations of the *set ipx network* command can be used to configure advanced RIP features and policies.

IPX RIP and SAP can be enabled or disabled for each remote site connection. You cannot individually enable or disable RIP or SAP; they are enabled or disabled together for each remote site connection. You can configure whether the OCR 812 should advertise local routes and services, only listen for routes and services from the remote site, or both.

- To configure IPX RIP and SAP for the remote site connection, use the command:

  ```
  set vc < vc name>
     ipx_routing [ALL |  LISTEN | NONE | RESPOND | SEND]
  ```

Bridging

A bridge connects two or more physical networks together to function as one big network. The OCR 812 can be configured to be a learning bridge. A learning bridge does more than just link networks; it separates network traffic and forwards only the packets that need to be forwarded.

Bridges separate traffic by examining the Media Access Control (MAC) addresses contained in data packets. MAC addresses uniquely identify each machine attached to a network segment. A data packet is not forwarded to another segment if its destination MAC address resides on the same segment as its source.

To efficiently separate traffic, the bridge maintains a Bridge Forwarding Table. The table contains a list of MAC addresses and their associated network segments. The table is built dynamically from the source MAC addresses of data packets passing through the bridge.

The OCR 812 bridge supports the Spanning Tree Protocol (STP). This feature is used when two networks are joined by two bridges forming a looped network. STP prevents the data packets from circling the two networks.

The OCR 812 provides a Bridge Firewall function which allows flexible configuration of simultaneous bridging and routing. For more information on the Bridge Firewall, see the **Bridging and Routing** section.

To set up bridging on the OCR 812, you must:

- Configure bridging for the LAN.
- Configure bridging for the remote site connection.

You may also want to:

- Set up to bridge IP traffic.
- Modify advanced bridging options.

Details are provided in the following sections.

*Remember to save your configuration using the **save all** command before rebooting your OCR 812 so that your changes will be written to permanent FLASH memory.*

Configuring Bridging for the LAN

To configure a protocol over the LAN, you need to assign a protocol network to the LAN port by providing a name. After adding a network, you can modify advanced parameters.

- To add a bridge network over the Ethernet interface, use the command:

  add bridge network <network name>

You can obtain a list of all configured networks using the command **list networks**.

To only list bridge networks, use **list bridge networks**.

- By default, the network is enabled when it is created. You can disable the network using the following command:

  disable bridge network <network name>
- You can delete a disabled network using the command:

  delete bridge network <network name>

Configuring Bridging for the Remote Site Connections

To configure bridging to a remote site you must enable bridging in the VC profile using the command:

```
set vc <vc name>
  bridge [DISABLE | ENABLE]
```

Bridging IP Traffic

By default the OCR 812 is set up to route IP traffic. To bridge IP traffic you must turn off IP Forwarding.

IP Forwarding refers to the routing of IP packets from one interface to another. It does not affect communicating to the OCR 812 itself. Even when IP Forwarding is disabled, you can perform non-routing functions such as use a Web browser to manage the unit and use PING.

- To see the current IP Forwarding status use the command:

  show ip settings
- To disable IP Forwarding use the command:

  disable ip forwarding

Advanced Bridging Options

The advanced bridging configuration options include Aging Time, Forward Delay, Spanning Tree, and Spanning Tree Priority.

- To see the current settings for these options, use the command:

  show bridge settings

Except for enabling Spanning Tree, most users do not need to change the advanced parameters from their default settings

The Aging Time is the time (in seconds) for aging out forwarding table information.

- To change the Aging Time, use the command:

  set bridge aging_time <seconds>

The Forward Delay is the time (in seconds) to wait while learning forwarding information before starting to bridge packets.

- To change the Forwarding Delay, use the command:

  set bridge forward_delay <seconds>

Spanning Tree refers to the Spanning Tree Protocol which is used to eliminate network loops between bridges.

- To disable or enable Spanning Tree, use the commands:

  disable bridge spanning_tree

  enable bridge spanning_tree

The Spanning Tree Priority is the priority assigned to a bridge that is running the Spanning Tree Protocol. It is used for prioritizing the bridges when Spanning Tree is enabled.

- To change the Spanning Tree Priority, use the command:

  set bridge spanning_tree_priority <priority value>

MAC-Encapsulated Routing

Because routers base their forwarding decision on network-level addresses, packets that are routed over a WAN are transmitted without MAC-layer addresses. Additionally, address resolution procedures that can be used to determine the destination MAC address for a packet are not required.

Conversely, packets that are bridged over a Wide Area Connection include MAC-layer information. Address resolution procedures are required.

MAC-Encapsulated Routing uses network-level addresses for forwarding decisions but transmits MAC-layer addresses over the Wide Area Connection. Additionally, address resolution procedures are used. To the remote site, the packets appear as if they had been bridged.

This feature allows the routing features of the OCR 812 (i.e., address translation, DHCP Server, DNS Proxy, etc.) to be employed in a bridged environment.

Configuring MAC-Encapsulated Routing

MAC-Encapsulated Routing is specified on a per-VC basis. When MAC-Encapsulated Routing is enabled in a VC profile, packets for the routed protocols configured by the profile (i.e., IP and/or IPX) will be sent using the appropriate bridged encapsulation. If the configured network service is RFC 1483, then the packets will be encapsulated in a bridged-1483 format. If the configured service is PPP, the packets will be encapsulated in BRCP.

- To enable MAC-Encapsulated Routing in a VC profile, use the command:

  set vc <vc_name> **mac_routing enable**

- To disable the MAC-Encapsulated Routing in a VC profile, use the command:

  set vc <vc_name> **mac_routing disable**

Simultaneous Bridging and Routing

The OCR 812 can be configured for simultaneous bridging and routing. IP routing is configured if IP forwarding is enabled (see Enabling IP Routing). IPX routing is enabled if an IPX network is present over the Ethernet interface (see Configuring IPX for the LAN). Bridging is enabled by adding a bridge network over the Ethernet interface. (see Configuring Bridging for the LAN). Routing and bridging are enabled for each destination in its remote site profile.

When configured for simultaneous bridging and routing, packets received from the LAN are first passed through the router for any configured protocols. If the packet can not be routed it is passed to the bridge depending on the setting of the Bridge Firewall function.

The Bridge Firewall has three modes:

1 Discard Routed Protocols:

This is the default mode. If a protocol is configured for routing and a packet for that protocol type is received from the LAN that is not addressed to the MAC address of the OCR 812, it is discarded. Additionally, broadcasts (including ARPs) for the protocol are not passed to the bridge. To configure the Bridge Firewall for this mode, use the command:

set bridge firewall discard_routed_protocols

2 Forward Unicast Packets Only:

If a protocol is configured for routing, and a packet for that protocol type is received from the LAN that is not addressed to the MAC address of the OCR 812, it is bridged. Additionally, ARP broadcasts for IP addresses other than that of the OCR 812 are also bridged. Other broadcasts for the configured protocol are not bridged. To configure the Bridge Firewall for this mode, use the command:

set bridge firewall fwd_unicast_only

3 Forward Broadcast/Unicast Packets:

Unicast packets for a configured protocol received from the LAN that are not addressed to the MAC address of the OCR 812 are bridged. Received broadcasts (e.g., DHCP) are bridged. To configure the Bridge Firewall for this mode, use the command:

set bridge firewall fwd_bc_and_unicast

Packets received from the WAN do not pass through the Bridge Firewall. Instead, packets received from the WAN are delivered to the router or bridging function based on their encapsulation and on the state of the MAC-Encapsulated Routing parameter in the remote site profile.

In general, a packet received in a routed encapsulation (i.e., IPCP or Routed RFC 1483) is delivered to the router. A packet received in a bridged encapsulation is passed on to the bridge. If MAC-Encapsulated Routing is enabled, the received (bridge-encapsulated) packets are delivered to the router.

System Administration

This section provides details and examples for performing the following system administration tasks:

- Setting Date and Time
- Setting System Identification
- Configuring Web Browser and TELNET Login Access
- Providing TFTP Access
- Setting Password Protection

*Remember to save your configuration using the **save all** command before rebooting your OCR 812 so that your changes will be written to permanent FLASH memory.*

Setting Date and Time

Date and time values are automatically set when the OCR 812 powers-up. *Optionally*, CLI commands can be used to manually set these values.

To manually set the **date**, use the command **set date** (which sets the system date, and leaves the time unchanged).

- **Set date** command format is dd-mmm-yyyy.
- Month (mmm) must be specified as the first three characters of the month name.

- Year (yyy) can be specified as 2 digits or as 4 digits (97 or 1997).

  For example: **set date 01-JAN-1998**

To manually set the **time**, use the command **set time** (which sets the system time, and leaves the date unchanged).

- **Set time** command format is hh:mm:ss.
- The seconds (ss) field is optional.
- Military time (GMT in 24-hour format) is used.

  For example:

  - To set the time to 4:10 **am**, enter the command **set time 04:10**.
  - To set the time to 4:10 **pm**, enter the command **set time 16:10**.

Date and Time values are for the current session only.

Setting Date and Time Using Network Time Protocol (NTP)

The OCR 812 supports use of the Network Time Protocol (NTP) to automatically set system date and system time to the values provided by NTP servers installed on the network.

- The default setting for NTP is **enabled**.

  The OCR 812 maintains a list of known NTP servers installed on the network. If a particular NTP server is not specified, the OCR 812 randomly selects two NTP servers from the list and designates them primary NTP server and secondary NTP server (respectively).

- If an installed NTP server is not available on your network, the OCR 812 sets system date and time using the values automatically provided at system power-up, or the values set manually by the user with CLI commands.

Network Time Protocol CLI Commands

- To enable NTP, use the following command:

  set enable ntp

  If the system detects the presence of an on-board Real-Time Clock (a battery powered chip ***not*** installed in Release 2.0 OCR 812 units), the default is **disable** ntp; otherwise, the default is **enable** ntp.

- To disable NTP, use the following command:

  set disable ntp

- To specify a primary NTP server, use the following command:

  set primary_server <ip_name_or_addr>

  <ip_name_or_addr> is the IP address or host name of the *primary* server the OCR 812 queries for date and time information/synchronization.

  The primary server is randomly selected from a list of known NTP servers you can access on the Internet at www.ntp.org. Many of these NTP servers can be used free of charge. To view a sample list of NTP servers, please see NTP Servers List.

If more than one OCR 812 is installed in your network, each OCR 812 is assigned a *different* primary NTP server (the assignment of a primary NTP server to a given OCR 812 is based on the unique MAC address of that OCR 812 unit).

- To specify a secondary NTP server, use the following command:

  set secondary_server <ip_name_or_addr>

  <ip_name_or_addr> is the IP address or host name of the *secondary* server the OCR 812 queries for date and time information/synchronization whenever the *primary* server is unavailable.

  The secondary server is randomly selected from a list of known NTP servers you can access on the Internet at www.ntp.org. Many of these NTP servers can be used free of charge. To view a sample list of NTP servers, please see NTP Servers List.

  If more than one OCR 812 is installed in your network, each OCR 812 is assigned a *different* secondary NTP server (the assignment of a secondary NTP server to a given OCR 812 is based on the unique MAC address of that OCR 812 unit).

- To specify an NTP server polling interval, use the following command:

  set polling_interval <seconds>

  <seconds> is the polling interval used by the NTP process to gather time synchronization information. The range available is 64 seconds to 1024 seconds (approximately 18 minutes).

  The default polling interval is 600 seconds (10 minutes).

- To specify an NTP server maximum retransmission value, use the following command:

  set retransmissions <number>

  <number> is the maximum number of times a request will be re-transmitted to a given server before the server is considered unavailable.

  The value for <number> can be any value from 1 through 200, inclusive.

  The default maximum value for <number> is five.

- To specify an NTP server retransmission timeout value, use the following command:

  set timeout <seconds>

  <seconds> is the number of seconds since a request was last sent to a server. When elapsed time becomes *greater* than the value specified for <seconds>, the request times out.

  The value for <seconds> can be any value from 1 through 60, inclusive.

  The default value for <seconds> is ten.

- To specify a time zone for NTP, use the following command:

  set timezone <timezone_name>

  The default time zone is GMT.

- To display NTP time zone settings, use the following command:

  list timezone

- To display NTP settings, use the following command:

  show ntp <settings>

- To display NTP counter values, use the following command:

  show ntp counters

NTP Servers List

The following is a *partial* list of available NTP servers that can be found at the www.ntp.org web site. For an up-to-date, comprehensive list of all available NTP servers, please visit www.ntp.org.

NTP Servers

```
"clock.psu.edu"                      /* Penn State Univ. */
"clock.tricity.wsu.edu"              /* Wash. State Univ. */
"gilbreth.ecn.purdue.edu"            /* Purdue Univ. */
"constellation.ecn.uoknor.edu"       /* Univ. of Oklahoma */
"harbor.ecn.purdue.edu"              /* Purdue Univ. */
"libra.rice.edu"                     /* Rice Univ. */
"louie.udel.edu"                     /* Univ. of Delaware */
"molecule.ecn.purdue.edu"            /* Purdue Univ. */
"ntp.cox.smu.edu"                    /* Southern Methodist Univ. */
"ntp.cmr.gov"                        /* Center for Seismic Studies */
"ntp.ctr.columbia.edu"               /* Columbia Univ. */
"ntp.tmc.edu"                        /* Baylor College of Medicine */
"ntp1.cs.wisc.edu"                   /* Univ. of Wisconsin */
"ntp0.cornell.edu"                   /* Cornell Univ. */
"ntp-1.cso.uiuc.edu"                 /* Univ. of Illinois */
"ntp5.tamu.edu"                      /* Texas A&M Univ. */
"ntp-1.vt.edu"                       /* Virginia Tech Computing Center */
"sundial.columbia.edu"               /* Columbia Univ. */
"tock.cs.unlv.edu"                   /* Univ. of Nevada */
"timex.cs.columbia.edu"              /* Columbia Univ. */
"wuarchive.wustl.edu"                /* Washington Univ. */
```

Displaying Date, Time, and System Uptime

To display current date, current time, and system uptime (time elapsed since power-on), use the command **show date**.

Date and time information displays in the following format:

```
System Date:        02-MAR-1998 05:17:00
System UpTime:      2d 08:37:54
```

Setting System Identification

The system name, location and contact information is useful when monitoring the OCR 812 remotely. You should choose a name, location and contact that is appropriate for the unit.

- You can view the settings using the command:

  show system.
- To set these parameters use the command:

  set system name <name> **location** <location> **contact** <contact>
- The name, location, and contact can be up to 32 characters long. For example,

  set system name OCR1 **location** Rack4 **contact** SysAdmin@555-1212

You must assign a system name to the OCR 812 using the ***SET SYSTEM NAME <name>*** *command. If you do not assign a system name, the unit may reboot during PPP operation.*

Configuring Web Browser and TELNET Login Access

Setting up a login user allows you to provide controlled access to the OCR 812 from a Web browser or through TELNET. Connecting with a Web browser allows you to configure and monitor your unit using the OCR 812 Manager. Connecting using TELNET on a workstation allows you to remotely manage the unit using CLI.

A default user name of **root** and password **!root** are provided by DHCP Smart Mode and the IP Wizard during the initial installation. For secure access, you should add a private login name and password and delete the default name.

- To view the current login users, use the command:

  list users
- To add a login user, use the command:

  add user <name> **password** <password>

The name can be up to 32 characters long and the password can be up to 15 characters long.

- To delete a login user, use the command:

  delete user <name>
- To change the password, use the command:

  set user <name> **password** <new password>
- To enable the use of CLI for TELNET users, issue the additional command:

  enable security_option remote_user administration

Providing TFTP Access

Trivial File Transfer Protocol (TFTP) provides a simple way to transfer files from one machine to another. The OCR 812 has a TFTP server that allows you to copy files to or from the unit. All you have to do is set up TFTP access on the OCR 812 and run a TFTP client program on a workstation.

You can configure the OCR 812 to provide access to all TFTP clients or you can specify the IP addresses of the TFTP clients for restricted access.

- To view the current TFTP client access list, use the command:

  list tftp clients
- To add a TFTP client to the list, use the command:

  add tftp client <host name or IP address or 0.0.0.0>

Provide either the host name or the IP address of the workstation running the TFTP client. An address of 0.0.0.0 allows all TFTP clients unrestricted access.

- To remove a TFTP client from the list, use the command:

  delete tftp client <host name or IP address or 0.0.0.0>

Setting Password Protection

The OCR 812 provides the capability to password-protect access to the CLI. When the password protection feature is enabled, a user connecting to the CLI via the serial console port will be prompted for the CLI password.

After the correct password is entered, all CLI commands are accessible by the user. The user can 'exit' from the CLI to disable further access or can configure an idle timeout period. If no commands are executed by the CLI for a period longer than the idle timeout period, the user will automatically be logged out of the console. The password will have to be re-entered in order to access the CLI again.

CLI password protection is **disabled** by default.

Password protection can be configured by the QuickSetup program or by using CLI commands.

The Console password is independent of the Login Access passwords. Only the Console password can be used to gain access to the Console port.

- To enable or disable CLI password protection, use the commands:

  enable command password <password> *or*
  disable command password

  where <***password***> is an alphanumeric string of 1 to 8 characters. The default password is “password.”
- To display console port *status* (console port connection *up* or *not up*), you can display console port *prompt* status by entering the **show command** command.

  For a description of the **show command** command, see Appendix B, show command.

Be sure to save your configuration after entering a new password.

- After logging in to the CLI, you can exit the CLI with the command:

  exit cli

- To set the idle timeout period, use the command:

  set command idle_timeout <timeout> where <*timeout*> specifies the idle timeout period in minutes. By default, there is no idle timeout period.

  This capability is useful for system administrators or users who wish to restrict access to the OCR 812.

Care should be taken to remember the configured password. If the password is forgotten, the unit must be sent back to 3Com support to have the feature disabled.

OfficeConnect Remote 812 Filtering Capabilities

The OCR 812 provides an extensive set of data and call filtering capabilities. The OCR 812 supports the following filtering capabilities:

- Input and output data filtering.
- Source and destination address filtering.
- Protocol filtering.
- Source and destination port filtering. A packet filter can control what services local or remote users can access.
- Route filtering can filter source and destination addresses in packets that exchange routing table information.
- Established session filtering. A packet filter can permit users to connect with a remote network without letting remote users have access to the local network (or vice versa).

Data Filtering Overview

The OCR 812 provides an extensive set of data filtering capabilities. For instance, filters can accept packets only from specific addresses to provide added security, or filters can be added to reduce network traffic and improve overall performance.

Packet filters control inter-network data transmission by accepting or rejecting the passage of specific packets through network interfaces based on packet header information. When data packets are received by a network interface such as an Ethernet (LAN) or WAN port, a packet filter analyzes the packet information using a set of rules you define. A filter then lets the packet pass through or discards it.

This chapter contains information on the filtering capabilities for your OCR 812 and is organized into the following sections:

- OfficeConnect Remote 812 Filtering Capabilities
- Creating Filters
- Assigning Filters
- Applying Filters
- Managing Filters

Filters can provide added security by accepting packets only from specific addresses or they can be added to reduce network traffic and improve overall performance. Filters can also be used to approximate spoofing when routers with different or incompatible spoofing methods are linked over the WAN. Spoofing is the use of a forged IP source address to circumvent a firewall.

Packet filters control inter-network data transmission by accepting or rejecting the passage of specific packets through network interfaces based on packet header information. When data packets are received by a network interface such as an Ethernet LAN or WAN port, a packet filter analyzes packet header information against a set of rules you define. A filter then lets the packet pass through or discards it.

Filter Classes

The OCR 812 supports three filter classes:

- **Input data** - filter packets as they enter.
- **Output data** - filter packets as they exit.
- **Embedded bypass** for periodic router protocol packets (IP RIP, IPX RIP and IPX SAP)

Each filter class can be identified further by the following types:

Filter Types

Filters can be classified by the following types:

- **Data filters** - based on protocol-specific packet information.
- **Advertisement filters** - based on broadcast packet information (IP RIP, IPX RIP, and IPX SAP).
- **Generic filters** - based on packet structure.

Data Filters

Data filters control network access based on the protocol, source / destination address, and port designation (e.g., TCP and UDP port designations) of the packet. The following table describes the data filters supported.

Table 6-3 Data Filters

Filter	Action
IP	Controls network access based on the protocol and source/destination address. IP filter rules allow filtering based on the source address, destination address, protocol type, source port, and port designation of the IP packet.
IPX	Controls network access based on the protocol and source/destination network. IPX filter rules allow filtering based on the source network, destination network, protocol type, source socket, destination socket, source node, and node designation of the IPX packet.
Bridge	Controls network access based on the source and destination MAC addresses.

Advertisement Filters

Advertisement filters operate on network protocol packets that contain varying information such as SAP or RIP. Filtering of these packets is performed by the specific protocol process.

The following table describes the advertisement filters supported:.

Table 0-1 Advertisement Filters

Filter	Action
IP-RIP	Controls the content of IP Routing Information Protocol (RIP) packets that are sent out or received on specific ports. The IP RIP filtering process filters addresses from the RIP packet upon transmission, and does not enter routes into the routing table upon receipt.

IPX-SAP	Controls the content of Service Advertising Protocol (SAP) packets that are sent out or received on specific ports. The IPX-SAP filter rules allow filtering on service type, server name, network address, node address, and socket number fields of the service entry. The forwarding process uses the filter information to prevent the service information from being included in the SAP packet.
IPX-RIP	Controls the content IPX RIP packets that are sent out or received on specific ports. The IPX RIP filtering process filters addresses from the RIP packet upon transmission, and does not enter routes into the routing table upon receipt.

Generic Filters

Generic filters are protocol-independent and are specified by byte and offset values in a packet. Packets are filtered by comparing each packet's offset value and byte information with the values that you define in the filter. The router will accept or reject the packet based on the result.

Creating generic filters can be a complex task. Only experienced users should employ generic filters, and strictly in cases where data and advertising filters cannot provide the filtering capabilities that you require.

Creating Filters Overview

Filters can be set using either the CLI or the OCR 812 Manager.

The more flexible way of setting filters is through the Command Line Interface (CLI). Both data and advertisement filters can be set using CLI. For more information on accessing CLI, *see* Chapter 1, Establishing Communications with the OfficeConnect Remote 812.

Data Filters can be set using the HTML Manager (the OCR 812 Manager). Data filters are used to remove packets from the normal flow of data traffic. They can be applied to IP, IPX, and/or Bridge traffic. Advertisement filters are used to restrict information in outgoing or incoming advertisement packets, i.e. IP RIP, IPX RIP, and IPX SAP packets.

Creating Filters Using Command Line Interface

Before creating a filter file, you should carefully identify the information you want to filter. Decide if you want a filter that discards packets (such as reject all IP packets whose IP source address is 192.168.200.50) or accept only a subset of packets (such as accept only bridged packets if the destination MAC address is 002069000001 or 002069000002). Also determine where you want to place the filter. For example, figure out if you want to apply the filter to packets coming into the Ethernet port, to packets going out the WAN (ATM) port, or to packets coming from a specific VC/remote site.

The first step in creating a filter on the OCR 812 is to create a file using a text editor on a workstation. The file will contain filters defined in the OCR 812 filter syntax (described below). File names should be short and descriptive, such as IP.FLT.

The next step is to use TFTP (Trivial File Transfer Protocol) to copy the filter file from the workstation to the OCR 812.

You then use CLI commands to add the filter file to the list of filters and apply the filter to the appropriate interface or VC / remote site profile.

Filter File Components in CLI

You define the filtering rules used by the router within filter files. Filter files are text files that are stored in the unit's FLASH memory. You can create and modify filter files using an off-line text editor, then TFTPing the finished file on to the unit.

To be valid, a filter file must always have the following file descriptor on the first line: **#filter**

Be sure that no blank space precedes the descriptor, or an error will occur.

The remainder of the filter file is partitioned into protocol sections. Each protocol section has a descriptive header and contains the filter rules for that protocol.

Protocol Sections

A single filter file can contain all valid protocol sections in any order, but the sections cannot be repeated. The following conditions will generate errors or prevent normal filter operation:

- If you do not specify a protocol section in the filter file, no filtering will occur and packets of that protocol type will be accepted.
- If you specify a protocol section but do not define any rules, an error will occur. The following table describes the valid protocol sections that you can define in the filter file.

To comment out a protocol section, you must place a pound (#) sign before the section header and before all rules defined in the section.

Table 6-4 Protocol Sections

Protocol Sections	**Descriptions**
IP	IP protocol data filter section
IP-RIP	IP RIP advertising filter section
IPX	IPX protocol data filter section
IPX-RIP	IPX RIP advertising filter section
IPX-SAP	IPX SAP advertising filter section
BR-ETH	Bridge protocol data filter

Protocol Rules

You can define protocol rules within each protocol section in the filter file. Protocol rules determine which packets may and may not access the network. The rule syntax is:

<line #> <verb> <keyword> <operator> <value>

The line # range is 1-10. This means you can combine up to 10 rules to create a filter for a specific protocol. Additionally, line number 999 is used for the DENY verb.

The combination of keyword, operator, and value forms the condition which (when combined with the verb) determines whether a packet is accepted or rejected.

When a packet is filtered, the router parses each rule defined in the protocol section sequentially according to the line number. *Filtering is performed based on* *the first match that occurs*. If there is no match, by default the packet is accepted. For this reason, you should order your protocol rules so that the rules you expect to be most frequently matched are in the beginning of the section. This reduces the amount of parsing time that occurs during filtering.

The following table describes each field used in the rule syntax:

Table 6-5 Protocol Rules

Field	Description
line #	Each rule must have a unique line number from 1-10 plus 999 for the DENY verb. You must arrange rules in increasing order.
Verb	This field can be one of the following: **ACCEPT** - Allow the packet access if the condition is met (use with DENY verb to indicate reject all other packets). **REJECT** - Do not allow the packet access if the condition is met. **AND** - Logically use the AND condition with condition of the next rule to determine if the packet is accepted or rejected. Both defined conditions must be met.
Keyword	The keywords for all protocol, descriptions, corresponding operators and values.
Operator	Describes the relationship between the keyword and its value. The operator field must be one of the following: = Equal != Not equal > Greater than < Less than >= Greater or Equal <= Less or Equal => Generic
value	Contains a entity that is appropriate for the keyword.

*The **OR** operation can be implemented by successive rules.*

For example, to accept a packet if the source address is xxx, or the destination address is yyy, the following rules are used (this will only accept packets from the specified address(es); all other packets will be rejected):

IP:
1 ACCEPT src-addr=xxx;
2 ACCEPT dst-addr=yyy;
999 DENY;

The following table describes the keywords for each protocol section and their legal operators used in the rule syntax.

Value ranges are also given where ddd is a decimal between 1 and 255, mask is a decimal between 1 and 32, and xx is a hex number:

Table 6-6 Protocol Keywords

Protocol Section	Keyword	Operators	Description and Value Range
IP	src-addr dst-addr tcp-src-port tcp-dst-port udp-src-port udp-dst-port protocol generic	=, != =, != all all all all =, != =	Source IP Address (ddd.ddd.ddd.ddd/mask) Destination IP Address (ddd.ddd.ddd.ddd/mask) TCP source port (1 - 65535) TCP destination port (1 - 65535) UDP source port (1-65535) UDP destination port (1-65535) IP protocol (UDP, TCP, ICMP) Generic filter
IP-RIP	network	=, !=	IP network number (ddd.ddd.ddd.ddd/mask)
IPX	src-net dst-net src-host dst-host src-socket dst-socket generic	=, != =, != =, != =, != all all =	Source IPX network (xx-xx-xx-xx) Destination IPX network (xx-xx-xx-xx) Source IPX host node address (xx-xx-xx-xx-xx-xx) Destination IPX host node address (xx-xx-xx-xx-xx-xx) Source IPX socket (0x1 - 0xFFFF) Destination IPX socket (0x1 - 0xFFFF) Generic Filter
IPX-RIP	network	=, !=	IPX network (xx-xx-xx-xx)
IPX-SAP	network node server service-type socket	=, != =, != =, != =, != all	IPX network (xx-xx-xx-xx) IPX node (xx-xx-xx-xx-xx-xx) Server name (character string to 32 characters) Service type (0x0 - 0xFFFF) Socket (0x1 - 0xFFFF)
BR-ETH	src-addr dst-addr generic	=, != =, != =	Source MAC address (xx-xx-xx-xx-xx-xx) Destination MAC address (xx-xx-xx-xx-xx-xx) Generic filter

Generic Filter Rule

The syntax for generic filters is slightly different than that for other filters:

```
<line #> <verb> GENERIC => ORIGIN = <FRAME > DATA>/OFFSET = <# of bytes>/
LENGTH = <# of bytes>/MASK = < 0x Mask>/VALUE = <0x value>
```

- **ORIGIN** - The location in the packet to start the offset count. This location can be at byte 0 (FRAME) or at the start of the protocol data (DATA).
- **OFFSET** - The number of bytes from the origin to skip before comparing the value to the packet contents.
- **LENGTH** - The number of bytes in the packet to compare to the value.
- **MASK** - The mask to logically "and" with the packet contents before comparing with the value (hex).
- **VALUE** - The value (hex) to compare to the packet contents.

For example, a generic bridge filter to prevent all IP packets from being bridged is:

```
BR-ETH:
1 reject generic=>origin=frame/offset=12/length=2/mask=0xFFFF/value=0x0800;
```

Applying the Rules Using CLI

The sections that follow provide detailed information and examples for creating specific filters based on protocol.

IP Source and Destination Network Filtering Using CLI

Source and destination address filtering is generally used to limit permitted access to trusted hosts and networks only, to explicitly deny access to hosts and networks that are not trusted, or to limit external access to a given host (for example, a web server or a firewall).

Note that only the part of the IP address specified by the mask field is used in the comparison. If a match is found, the packet is forwarded (rules containing accept) or discarded (rules containing reject).

The following rule example allows forwarding of **only** IP packets with source addresses that match the first 16 bits of the given IP address (addresses beginning with 192.77):

```
IP:
1 ACCEPT src-addr = 192.77.200.203/16;
999 DENY;
```

The following rule example rejects IP packets with a source address: 144.133.20.1.

```
IP:
1 REJECT src-addr =144.133.20.1;
```

The following rule example allows forwarding of only IP packets with source address 192.77.100.32 and destination address 201.128.11.34:

```
IP:
1 AND src-addr = 192.77.100.32;
2 ACCEPT dst-addr = 201.128.11.34;
999 DENY;
```

IP Source and Destination Port Filtering Using CLI

You can also filter against UDP and TCP ports. The following rule example rejects IP packets with a TCP port number of 80.

```
IP:
1 REJECT tcp_dst_port  = 80;
```

IP Protocol Filtering Using CLI

Filtering can be done on protocol as well. The protocols that can be filtered are UDP, TCP and ICMP. The following rule example rejects TCP packets.

```
IP:
1 REJECT protocol = TCP;
```

IP RIP Packet Filtering Using CLI

Routing Information Protocol (RIP) packets are used to identify all attached networks as well as the number of router hops required to reach them. The responses are used to update a router's routing table

If the router is listening for, or broadcasting RIP messages, you should allow them to pass in the appropriate direction(s). You define IP RIP filtering rules in the IP-RIP protocol section of the filter file.

For example, if you want to filter all routes except the one specified by the IP network address 195.12.254.45, you would create this rule:

```
IP-RIP:
1 ACCEPT network = 195.12.254.45;
999 DENY;
```

This filter only allows the route 195.12.254.45 into the route table. All other routes are rejected.

Spurious RIP messages can disrupt your routing tables. If you are listening for RIP messages on a given interface, you may wish to consider filtering out RIP updates from untrusted networks.

IPX Source and Destination Network Filtering Using CLI

IPX network numbers must be specified as an network number no greater than 8-digits in hexadecimal format. The following rule example rejects IPX packets with a source address: 00-03-42-BF.

```
IPX:
1 REJECT src-net = 00-03-42-BF;
```

IPX Source and Destination Host Filtering Using CLI

Host addresses must consist of the 8-digit network number, followed by the four digit node number in hexadecimal format.

The following rule example accepts IPX packets with a destination address of 04-0B-43-AA:

```
IPX:
1 ACCEPT dest-host = 04-0B-43-AA;
999 DENY;
```

IPX Source and Destination Socket Number Filtering Using CLI

Sockets numbers represent communications interfaces that let an application access a network protocol by opening a socket and declaring a destination. Sockets are useful because they provide a simple way to direct an application onto the network.

You can compare the source or destination IPX socket number contained in the packet to the socket number defined in the filter rules. You must specify the type of the comparison.

For example, the following rule example accepts IPX packets with the IPX source socket number 0x001:

```
IPX:
1 ACCEPT src-socket = 0x001;
999 DENY;
```

IPX RIP Packet Filtering Using CLI

Routing Information Protocol (RIP) packets are used to identify all attached networks as well as the number of router hops required to reach them. The responses are used to update a router's routing table.

You define IPX RIP packet filtering rules in the IPX-RIP protocol section of the filter file. You can filter IPX RIP packets by network only.

The following rule example filters the route specified by the IPX network address 00-03-55-BF:

```
IPX-RIP:
1 REJECT network = 00-03-55-BF;
```

IPX SAP Packet Filtering Using CLI

SAP packets are used to identify the services and addresses of servers attached to the network. The responses are used to update a table in the router known as the Server Information Table.

You define IPX SAP packet filtering rules in the IPX-SAP protocol section of the filter file. You can filter SAP packets by network, node, server, service-type, and socket.

The following rule example accepts SAP services from the server name sales_1, with a socket number is less than 32:

```
IPX-SAP:
1 AND server = sales_1;
2 ACCEPT socket < 32;
999 DENY;
```

Bridge / Generic Filtering Using CLI

The rules in this filter file section are setup to allow bridging of only IP and IPX packets (assuming that all traffic is being bridged and that the IPX protocol is using Ethernet_II framing). To stop traffic in both directions, you can apply the filter as an input_filter on both the Ethernet and the WAN or User Profile interfaces. However, to improve efficiency over the WAN interface, it would be better to have the same type of filter applied on the equipment at the other side of the WAN to keep non-IP and IPX traffic off the WAN completely.

```
BR-ETH:
# Allow IP traffic
1 ACCEPT generic=>origin=FRAME/offset=12/length=2/mask=0xFFFF/value=0x0800;
# Allow ARP traffic
2 ACCEPT generic=>origin=FRAME/offset=12/length=2/mask=0xFFFF/value=0x0806;
# Allow IPX traffic
```

```
3 ACCEPT generic=>origin=FRAME/offset=12/length=2/mask=0xFFFF/value=0x8136;
4 ACCEPT generic=>origin=FRAME/offset=12/length=2/mask=0xFFFF/value=0x8137;
999  DENY;
```

Step by Step Guide to Creating Filter Files Using CLI

You can create filter files using any text editor. Once the file is created, use the Trivial File Transfer Protocol (TFTP) to place the filter file in the router FLASH memory.

To create a filter file using CLI:

1. Open a new text file. Enter the file descriptor on the first line: **#filter**
2. Enter a file section header followed by a colon for the protocol rules you want to define. For example, if you want to define IP filtering rules, enter the following section header: **IP:**
3. You can comment a section header out by placing a # sign before the section header. This is useful if you want to insert a placeholder for a protocol section you will define in the future.
4. Enter the protocol rules for the protocol section you are defining. Observe the following guidelines.
   - Begin each rule with a unique line number ranging from 1 - 10.
   - Arrange rules in increasing line number order within each protocol section.
   - Arrange rules so that the rules you expect to be matched most frequently are toward the top of the list
   - Delimit each rule with a semi-colon. Example:

     ```
     IP 1 ACCEPT src-addr = 128.100.33.1;
     2 ACCEPT dst-addr = 200.135.38.9;
     999 DENY;
     ```
5. Continue to define protocol rules for each protocol section you want to filter.
6. Inspect the file to ensure that it meets all filtering rules.
7. This step is important since you cannot edit the filter file from within the CLI. To edit the file, you must modify the it using a text editor, TFTP the modified file into the FLASH (replacing the original file) and verify the filter using the verify filter command.
8. Save the filter file using a 12.3 FLT extension. The filter file extension will allow you to differentiate the filter file from other files stored in the router FLASH memory.
9. You can use the list files command to ensure the filter file was successfully stored in the router FLASH memory.
10. Configure a PC as a Trivial File Transfer Protocol (TFTP) client of the router by entering **add TFTP client <hostname or IP address>**.

    To use CLI, see Chapter 1, Establishing Communications with the OfficeConnect Remote 812. *This section provides detailed instructions for connecting the console cable and communicating with the OCR 812 using a terminal emulator like Microsoft's HyperTerminal.*

11. From a machine that has access to the same network as the router, use a TFTP command to transfer the filter file to the router FLASH memory.

For example, from the workstation command line enter:

```
tftp <OfficeConnect Remote 812 IP address> put <filter filename>
```

12 The router does not recognize a filter file stored in its FLASH memory until you add it to the managed filter table. To notify the unit about the filter file for the first time, you must issue the CLI command **add filter <name>** to add the filter to the managed filter table. When the filter is added, the unit automatically verifies the filter file syntax. If you modified a file that had already been added, use the **delete filter <name>** command to remove the old file before TFTPing the new file. Then use the **add filter <name>** command again.

13 If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, error messages are generated detailing the source of the errors.

14 Apply the filter to the appropriate interface or VC / remote site profile. After replacing a file, you need to re-apply the filter for it the new filter file to take effect.

For more details, refer to the next two sections. Assigning Filters discusses how to decide where to apply a filter, and Applying Filters Using CLI explains the appropriate CLI commands to use.

Assigning Filters

Once an input filter or output filter has been added to a router's list of managed filters, you can assign that filter to the unit's:

- Interfaces
- VC / Remote Site Profile
- VPN tunnel

Interface Filters

You can configure interface filters for any interface. Interface filters control access to all networks available for both modem and non-modem interfaces.

You can specify whether a filter applies to packets entering the interface (input filter) or leaving the interface (output filter). The router examines the filtering rules to determine whether the interface accepts or rejects the packet.

Input Filters

If an input filter is configured on an interface, all received packets are checked against the filtering rules before being forwarded to another interface.

Output Filters

If an output filter is configured on an interface, all outbound packets are checked against the filtering rules before exiting the router.

Input Filters vs. Output Filters

When possible, use the input filter to filter an incoming packet rather than waiting to catch a packet as it attempts to exit the router. This is recommended because:

- A packet is prevented from entering the router, keeping potential intruders from attacking the unit itself.
- The routing engine does not waste time processing a packet that is going to be discarded anyway.

- Most importantly, the router does not know which interface an outgoing packet came in through. If a potential intruder forges a packet with a false source address (in order to appear as a trusted host or network), there is no way for an output filter to tell if that packet came in through the wrong interface. An input filter, on the other hand, can filter out packets purporting to be from networks that are actually connected to a different interface.

VC/Remote Site Filters

You can configure filters for a specific VC / remote site profile that controls access to the network for that location. This filter is only applied for the duration of the remote network connection. As with interface filters, a remote site filter can be configured to apply to input or output data traffic. (Note that you can also assign filters (input and output) to your VPN tunnel).

Applying Filters Using CLI

You can apply filters to interfaces and/or users using the CLI. If you modify a file, you need to re-assign it to make the changes take effect immediately. Otherwise the changes will not take effect until the protocol network (IP, IPX, or bridge) that the filter affects goes down and comes back up. This occurs when a network is disabled, the WAN connection goes down then up, or when the OCR 812 is rebooted.

Do not apply a filter to more than one interface or VC / remote site profile. Also, do not apply an input and an output filter to more than one Ethernet interface.

Applying a Filter to an Interface Using CLI

To configure an input or output filter on an interface, use the following CLI commands:

```
set interface <interface name> input_filter <filter name>
set interface <interface name> output_filter <filter name>
```

Interface name is **eth:1** for the Ethernet interface and **atm:1** for the ATM interface. For example, to apply an input filter to the ethernet interface: **set interface eth:1 input_filter filter.fil**

*When assigning the filter to the Ethernet interface, you must turn off filter access by entering the CLI command **set interface eth:1 filter_access off.***

For more information about the filter access, refer to the **Setting Filter Access** section below.

Do not apply a filter to more than one interface or VC / remote site profile. Also, do not apply an input and an output filter to more than one Ethernet interface.

Configuring a Filter for a VC/Remote Site Using CLI

Do not apply a filter to more than one interface or VC/remote site profile.

To configure an input or output filter for a specific user, use the following commands:

```
set vc <vc or remote site name>input_filter <filter_name>
set vc <vc or remote site name>output_filter <filter_name>
```

For example, to apply an output filter to a user: **set vc corpoffice input_filter filter.fil**

Configuring Filters for a VPN Tunnel

To configure filters for a VPN tunnel, use the following commands:

```
set tunnel <tunnel name> input_filter <filter_name>
set tunnel <tunnel name> output_filter <filter_name>
```

For more information about configuring a VPN Tunnel (including information about configuring filters), see Setting Up a Virtual Private Network (VPN) Tunnel, Creating a VPN Tunnel Using 812 Default Values, and Tunnel Commands.

Setting Filter Access Using CLI

When filters are assigned to both the WAN interface and a VC/remote site profile, you need to tell the router which one to use using the filter access parameter. If filter access is ON, the VC / remote site filters will override interface filters. If filter access is OFF, then the interface filters are used.

Always turn filter access OFF for the Ethernet interface since there are no profiles associated with it. If you do not turn if off, the filter will not be applied.

To set the filter access parameter to ON for a specific interface, use the CLI command

```
set interface <interface_name> filter_access ON
```

To set the filter access parameter to OFF for a specific interface, use the CLI command

```
set interface <interface_name> filter_access OFF
```

Managing Filters Using CLI

This section provides information about how to perform filter management tasks.

Displaying the Managed Filter List Using CLI

To display the list of managed filters, use the following command:

```
list filters <filter_name>
```

The resulting display might look like this:

```
Filter Name         Status       Protocols
 ip.fil             NORMAL       IP IP-RIP
```

Adding Filters to the Managed List Using CLI

The **add filter** command verifies filter syntax prior to adding the filter to the managed list. If the syntax is valid, no message is generated and the command prompt returns. If syntax errors exist, error messages are generated detailing the cause of the errors.

If the syntax is invalid, the filter is still added to the managed list with a status of verify failed. To correct filter file errors, you must make the changes to the original filter file using a text editor, and re-TFTP the file to the router’s FLASH memory.

Then use the **verify filter** command to check the filter file syntax.

To add a filter file to the list of managed filters, use the CLI command

```
add filter <filter name>
```

It may be helpful to use the **list files** command to see files successfully stored in the FLASH memory.

Removing a Filter from an Interface Using CLI

To remove a filter that is assigned to an interface, use the following command:

```
set interface <interface name> input_filter ""
set interface <interface name> output_filter ""
```

The " " value represents a null value and removes the defined filter from the interface. For example, to remove an output filter from an interface named eth:1, you would use the following command:

```
set interface eth:1 output_filter ""
```

Removing a Filter from a VC/Remote Site Profile Using CLI

To remove a filter that is assigned to a remote site profile, use the following command:

```
set vc <VC or remote site name> input_filter ""output_filter ""
```

The " " value represents a null value and removes the defined filter from the user profile. For example, to remove an input filter from a VC / remote site profile named corpoffice, you would use the CLI command:

```
set vc corpoffice input_filter ""
```

Deleting a Packet Filter Using CLI

To delete a specific packet filter (removing the filter file permanently from the FLASH memory), use the following CLI command

```
delete filter <filter_name>
```

Deleting a Tunnel Filter Using CLI

To delete a specific tunnel filter, use the following CLI command:

```
set tunnel <tunnel name> input_filter ""output_filter""
```

Verifying Filter File Syntax Using CLI

The verify filter command must be used if you make changes to a filter file that has already been added to the managed list and re-TFTP it back to the router’s FLASH memory (using the same filename). The verify filter file will check the filter syntax. If the syntax is valid, no message is generated and the command prompt returns. If the syntax is not valid, error messages are generated detailing the source of the errors.

To verify a filter file, use the CLI command

```
verify filter <filter_name>
```

Showing Filter File Contents Using CLI

To view the contents of an entire filter file that has been added to the managed list of filters, use this command:

```
show filter <filter_name>
```

To display the contents of the filter file by protocol, use the CLI command

```
show filter <filter_name> protocol BR-ETH | IP | IP-RIP | IPX | IPX-RIP | IPX-SAP
```

A

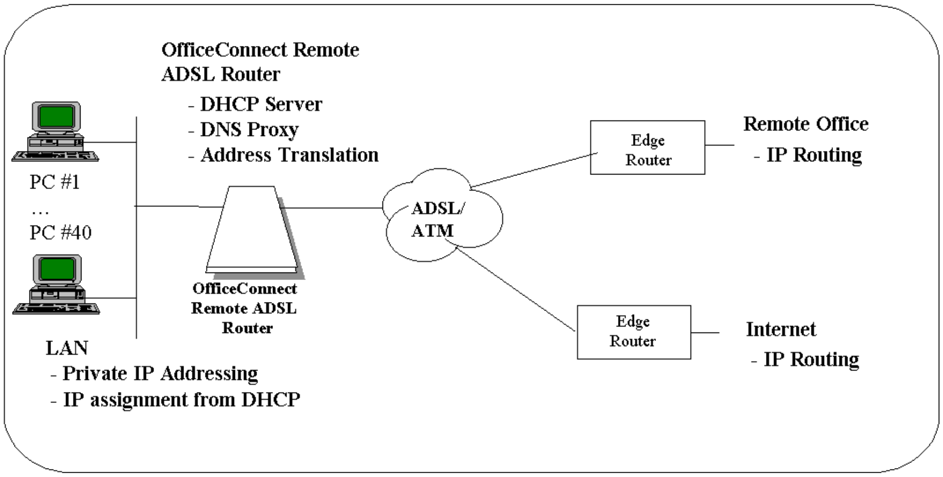
OFFICECONNECT REMOTE 812 SAMPLE CONFIGURATION

Sample Configuration Overview

This section describes a sample configuration that illustrates the following OCR 812 features:

- Address Translation
- Internal DHCP Server and DNS Proxy.
- Multiple Remote Sites, with different routing and bridging configurations.

Our sample SOHO network, shown below, has the OCR 812 connected to a LAN that is using private IP addresses. The OCR 812 is configured as the DHCP Server, dynamically assigning IP addresses and configuration information to each locally connected workstation. Two Remote Sites are defined, one to an ISP for Internet access, and another to the main Corporate office. IP routing is enabled for the Internet site and both IP and IPX routing as well as bridging is enabled for the Corporate site.



*Remember to save your configuration using the **save all** command before rebooting your OCR 812 so that your changes will be written to permanent FLASH memory.*

Configuring the Sample Network

The following sections discuss the six steps required to configure our sample network.

- Global Configuration
- IP LAN Network
- DHCP and DNS
- IPX LAN Network
- Bridge LAN Network
- Remote Sites

Global Configuration

Global configuration includes some optional "system" commands to identify the OCR 812's name, location, and support contact.   Next the Remote access security option is enabled to allow remote CLI access using TELNET. Finally, a Remote Login User is defined to provide access for Web Browser based management and TELNET. The following commands are executed:

```
set system name OfficeConnect_1

set system location Vienna

set system contact John_Doe

enable security_option remote_user administration

add user root password !root
```

LAN IP Network Configuration

A IP network is defined over the interface with the private address, 192.168.200.254 with a class C subnet mask. The IP network is identified by the name "ip" and uses Ethernet II framing. TFTP access is allowed for all clients. The following commands are executed:

```
add ip network ip address 192.168.200.254/C  frame ethernet_ii enable yes

add tftp client 0.0.0.0

enable ip forwarding
```

DHCP and DNS Configuration

The OCR 812's DHCP and DNS functionality is enabled to simplify configuration of the workstation on the LAN. A DHCP Server is defined with an address pool, and the default router and the DNS Server addresses are set to the OCR 812's LAN address. The DNS proxy is enabled and a Host statement is added for the OCR 812 to simplify access from the Web Browser. Finally, a Remote Server is defined for the Corporate remote site and a default Remote Server is setup to be dynamically learned over the Internet remote site. The following commands are executed:

```
set dhcp mode server

set dhcp server start 192.168.200.1 end 192.168.200.40 mask 255.255.255.0

set dhcp server router 192.168.200.254
```

set dhcp server dns1 192.168.200.254 **dns2** 0.0.0.0

set dhcp server wins1 0.0.0.0 **wins2** 0.0.0.0

add dns host ocrdsl-3com.com **addr** 192.168.200.254

add dns server MyCorp.com **primary** 192.168.1.253

add dns server * **vc** Internet

enable dns

When a DNS request is received from a locally attached workstation, the OCR 812 will search the local static table to find an entry. If one is not found, the request will be forwarded to a Remote DNS Server. The DNS Server is selected by comparing the domain name within the Request.

If the Request was for www.MyCorp.com/events/local the domain MyCorp.com would match given our configuration and the request would be forwarded to the DNS Server at 192.168.1.253.

If a request was for www.3com.com, a match would not be found in the Remote server table and therefore the request would be forwarded to the default Remote DNS Server. In this case, the Remote DNS Server is dynamically learned when the connection to the remote site "Internet" is first established.

After a workstation is rebooted and is configured automatically by the OCR 812's DHCP Server, the 812's browser-based Manager can attach to the OCR 812 by typing in ocrdsl-3com.com in the Browser's location field. If the OCR 812's DNS functionality is disabled, the manager can still be accessed by using the OCR 812's LAN address (i.e., 192.168.200.254 for this configuration).

LAN IPX Network Configuration

The local IPX Network is defined with a Network Number of 10 and an identifying name of "ipx". Routes and Services will be dynamically learned using RIP and SAP once the Remote Site to MyCorp is established. The following commands are executed:

add ipx network ipx **address** 10 **frame** ethernet_ii **enable** yes

set ipx net ipx **rip** both **sap** both

Bridge Configuration

A Bridge network is configured for the LAN. With our example, IP and IPX are routed over the Corporate Remote Site and all other protocols (e.g. AppleTalk) will be bridged. The Bridge network is added with the following commands:

disable bridge spanning_tree

add bridge network bridge

Remote Site: Internet

In our example, we have two defined Remote Sites. In this section, the Remote Site to the ISP is defined with the identifying name of "Internet". The configured network service is PPP, our local WAN address and the remote router address will be dynamically learned when the connection is established. In addition, we will dynamically learn the addresses for two remote DNS Servers. The login name for this account is “internet-user” and the password is “1a2b3c”.

Port Address Translation will be enabled, allowing all the workstations on our local LAN to share one public IP address. This Remote Site will be used as our default gateway. The ATM virtual channel is VPI 0 and VCI 32 and the Peak Cell Rate is set to the default access rate.

This remote site is configured with the following commands:

```
add vc Internet

set vc Internet ip enable ipx disable bridging disable

set vc Internet network_service ppp

set vc Internet send_name internet-user send_password 1a2b3c

set vc Internet atm vpi 0 vci 32 category_of_service unspecified pcr 0

set vc Internet address_selection negotiate

set vc Internet local_ip_address 255.255.255.255

set vc Internet nat enable

set vc Internet ip_routing listen

set vc Internet default_route_option enable

enable vc Internet
```

Remote Site: Corporate Access

In this section, the Remote Site to the Corporate office is defined with the identifying name of “corp-net”. IP and IPX are both routed over this remote site and all other protocols are bridged. The configured network service is RFC 1483 and the remote router address is specified (192.168.1.254). The WAN IPX interface is Unnumbered.

Port Address Translation is disabled on this Remote Site Profile. The ATM virtual channel is VPI 0 and VCI 33 and the Peak Cell Rate is set to the default access rate. This remote site is configured with the following commands:

```
add vc corp-net

set vc corp-net ip enable ipx enable bridging enable

set vc corp-net network_service rfc_1483

set vc corp-net atm vpi 0 vci 33 category_of_service unspecified pcr 0

set vc corp-net remote_ip_address 192.168.1.254

set vc corp-net local_ip_address 0.0.0.0

set vc corp-net nat_option disable
```

set vc corp-net **ip_routing** both

set vc corp-net **ipx_address** 0 **ipx_routing** all

enable vc corp-net

B

CLI Command Description

CLI Commands

ADD

Use the ADD command to define:

- Networks you will connect to
- Hosts you need to access
- SNMP communities
- Users who will dial out, dial in, access the network, or use the CLI

Note that some parameters have default values.

add access <ip subnet address>

The access list defines which Remote IP Subnets are allowed access to the Management services of the OCR812. Use this command to add an entry to the list.

Parameter	Description
ip subnet address	IP address in the xx.xx.xx.xx/mask format.

add auto_filter eth_blk_dst

Automatically adds and enables a blocking destination subnet address on the Ethernet interface.

- **Address** - IP address of the subnet to be blocked.
- **Mask** - IP netmask of the subnet to be blocked.

add auto_filter vc_blk_netbios

Automatically adds and enables an input filter on the specified VC. The filter DP ports 137 and 138, and TCP ports 139 and 143.

- **VC** - Specified VC profile name.

add bridge network <network_name>

- **{ enabled [yes] }**

Defines a bridge network connection, so your LAN users can bridge to other LANs across the WAN. bridging is supported over the WAN.

Note that routing takes precedence over bridging, so that bridging will not occur unless you disable routing for the protocols you wish to bridge. The protocols to bridge, and other important parameters, are specified in the user you use to establish this connection.

You must use *add user* to create a network type user for this command, and *set user* to specify the protocol and other parameters related to bridging.

Parameter	Description
<network_name>	Designation you wish to give to this bridge network.
enabled	Default is to enable the bridge network.

add dns host <host_name> address <ip_address>

Adds the named host to the Local Host Table. When the system needs to resolve an address for an IP host name, the Local Host table is checked first, before a request is sent to the remote DNS Name Server.

The add login_host command may also add to this table. See that command's description for details.

Parameter	Description
<host_name>	Designation of the local host.
<ip_address>	IP address of a named host in nnn.nnn.nnn.nnn format.

add dns server <domain_name>

- **primary_address [ip_address]**
- **secondary_address [ip_address]**
- **vc_name [vc_name]**

Adds the IP address of a remote DNS Server for the specified Domain Name to the Domain Name Server Table. The first specified server is sent the IP host name to be resolved, first without, and then with the default domain name (see *set dns* for more information about the default domain name). If that server cannot resolve the name, it is sent to the next specified server. If PPP is being used for a wide area connection, the vc_name parameter to specify a remote connection from which the primary and secondary addresses will be learned.

Parameter	Description
<domain_name>	Domain name. Use * for all domains.
Status	The status concerning the DNS server.
primary_address	The primary IP address of the DNS server.
secondary_address	The secondary IP address of the DNS server.
vc_name	The VC profile to use for obtaining the DNS addresses

add filter <filter_name>

Adds a filter file name to the filter table. The filter table is a managed list of filter names used by SNMP. A filter file is a text file stored in the FLASH file system, that you load using TFTP. *Add filter* also verifies the syntax of the filter file.

If syntax verification fails, you'll receive an error message, and the filter will still be added to the table, but is not usable.

You must correct the filter file in a text editor, use TFTP to export the updated file to the system's FLASH file system, and use the *verify filter* command to check the filter's syntax.

Parameter	Description
<filter_name>	Designation of a filter file, up to twenty ASCII characters.

add framed_route vc <name>

- **ip_route [ip_address]**
- **metric [number]**

Adds a framed (static) network to the VC profile for WAN connections. This method of creating a static route does not run RIP to learn routes, so you must specify IP route and gateway addresses. See *add ip route.*

Parameter	Description
<VC profile name>	VC profile name specified for the framed network. This is limited to 32 characters.
ip_route	IP address of the remote network
metric	Integer representing how far away the route is, in "hops" from other routers. Values are 1 through 15.

add framed_route tunnel <tunnel_name>

- **ip_route [ip_address]**
- **metric [number]**

Adds a framed (static) network to the VC profile for WAN connections. This method of creating a static route does not run RIP to learn routes, so you must specify IP route and gateway addresses. See *add ip route.*

Parameter	Description
<VC profile name>	VC profile name specified for the framed network. This is limited to 32 characters.
ip_route	IP address of the remote network
metric	Integer representing how far away the route is, in "hops" from other routers. Values are 1 through 15.

*Before adding a framed route for a VPN tunnel, ensure that the tunnel is disabled. Once the tunnel has been disabled, you can then add the framed route using the **add framed_route** command.*

add ip defaultroute gateway <ip_address>

- **{ metric [1] }**

Defines a default gateway IP router, which acts as the default route for IP packets destined for remote hosts.

Parameter	Description
<IP_address >	IP address of the gateway router.
metric	Integer representing how far away the default router is, in "hops" through other routers. Values: 1-15.

add ip network <network_name>

- **address [ip_net_address]**
- **frame [ETHERNET_II | SNAP | LOOPBACK]**
- **{ interface [eth:1] }**
- **{ enabled [yes]** }

Adds an IP network to the list of IP networks available over the specified interface.

Parameter	Description
<network_name>	Name of IP network, consisting of up to 32 unique ASCII characters; space must be surrounded by double quotes.
address	IP address of the network, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The Mask Specifier can be 'A', 'B', 'C', or 'H', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If you do not specify a mask, the system will generate it for you from the network address.
frame	Frame encapsulation to be used on this IP network. The options are: ETHERNET_II, LOOPBACK (for diagnostics), or SNAP.
interface	Name of the interface which this IP network will communicate over. The default is the first LAN interface (eth:1).
enabled	This optional parameter indicates whether the network is enabled (YES) or disabled (NO). YES is the default.

add ip route <ip_net_address>

- **gateway [gateway_addr]**
- **metric [hop_count]**

Adds an entry to the IP routing table. IP packets destined for networks that match this network will be routed to this address. The command *list ip routes* displays your currently defined routes.

Parameter	Description
<net_address>	IP address of the remote network, in the format nnn.nnn.nnn.nnn, with or without a mask specifier. The Mask Specifier can be 'A', 'B', 'C', or 'H', or a numeric value from 8 to 30 that describes the number of one bits in the mask. If you do not specify a mask, the system will generate it from the network address.
gateway	IP address of gateway used to reach this remote network.
metric	An integer representing how far away the route is, in "hops" through other routers. Values are 1-15.

add ipx network <network_name>

- **address [ipx_address]**
- **{ interface [eth:1] }**
- **{ enabled [yes] }**
- **frame [ETHERNET_II | SNAP | DSAP | NOVELL_8023]**

Adds an IPX network to the list of IPX networks available over the specified interface.

Parameter	Description
<network_name>	Name of IPX network. A unique ASCII string of up to 32 characters; space must be surrounded by double quotes.

address	Address of the IPX network.
interface	Name of the interface with which this IPX network is to be associated. The default is the first LAN interface (*eth:1*).
enabled	Optional parameter indicates whether the network is enabled (YES) or disabled (NO) by this command. YES is the default.
frame	Frame encapsulation chosen for this IPX network.

add ipx route <ipx_net_address>

- **gateway [ipx_host_address]**
- **metric [metric_number]**
- **ticks [tick_number]**

Adds an IPX static route (for the LAN) to the system's IPX Route table, which defines static routes to remote IPX networks.

The command *list ipx routes* displays currently defined static routes.

Parameter	Description
<ipx_net_address>	IPX network address requiring a route.
gateway	IPX address of the host which will act as a gateway. The format is nnnn.xx:xx:xx:xx:xx:xx (net_addr.mac_address).
metric	Number of "hops" through different routers needed to reach the remote IPX network.
ticks	Estimated interval in ticks it takes to deliver a packet to the remote network. There are approximately 18 ticks per second.

add ipx service [service_name]

- **address [internal network number]**
- **gateway [network_number.mac_address]**
- **metric [metric]**
- **node [internal_node_number]**
- **socket [socket_number]**
- **type [service_type]**

Adds a static IPX service (for the LAN) to the IPX services table. You must supply the name, internal ipx network number, node number, socket, and type of service for this service. The user must also supply gateway information to indicate the next router hop. To remove this service, use the *delete ipx service* command.

Parameter	Description
service name	Designation of IPX service.
address	Internal network number for the IPX service on which this service resides.
Gateway	Address of the router you defined as the gateway.
metric	An integer representing how far away the default router is, in "hops" through other routers. Values: 1-15.
node	The internal MAC address of the server on which the service resides. This is typically 00:00:00:00:00:01.
type	Type of service: hex number referring to file server, print server, etc. Refer to the table below.
socket	Socket number that the service uses.

Below is a partial list of the IPX services available:

Type	Description
04	file server
05	job server
07	print server
09	archive server
0A	job queue
21	NAS SNA gateway
2E	dynamic SAP
47	advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES-NetWare VMS
98	NetWare access server
9A	Named Pipes server
9E	PortableNetWare-UNIX
107	NetWare 386
111	Test server
166	NetWare management
26A	NetWare management
26B	Time synchronization
278	NetWare Directory server

add ipx_route vc <name>

- **ipx_net [ipx_address]**
- **metric [hop_count]**
- **ticks [tick_number]**

Adds an IPX route for the a user over the WAN.

Parameter	Description
<name>	The name of the user for the IPX route.
Ipx_net	IPX address of the route, in IPX (xxxxxxxx) form.
Metric	An integer representing how far away the route is, in "hops" through other routers. Values are 1-15.
ticks	Estimated interval in ticks it takes to deliver a packet to the remote network. There are approximately 18 ticks per second.

add ipx_service vc <name>

- **ipx_net [ipx_address]**
- **hops [number]**
- **name [name]**
- **node [internal_node_number]**
- **socket [socket_number]**
- **type [service_type]**

Adds a static IPX service (for the WAN) to the IPX services table.

You must supply the name, internal ipx network number, node number, socket, and type of service for this service. The user must also supply gateway information to indicate the next router hop.

Parameter	Description
<name>	The name of the user for the IPX route.
Petitioned	IPX address of the route, in IPX (xxxxxxxx) form.
Hops	An integer representing how far away the route is, in “hops” through other routers. Values are 1-15.
name	Estimated interval in ticks it takes to deliver a packet to the remote network. There are approximately 18 ticks per second.
node	The internal MAC address of the server on which the service resides. This is typically 00:00:00:00:00:01.
socket	Indicates which “socket” the server listens on.
type	Type of service: hex number referring to file server, print server, etc. Refer to the table below.

Below is a partial list of the IPX services available:

Type	Description
04	file server
05	job server
07	print server
09	archive server
0A	job queue
21	NAS SNA gateway
2E	dynamic SAP
47	advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES-NetWare VMS
98	NetWare access server
9A	Named Pipes server
9E	PortableNetWare-UNIX
107	NetWare 386
111	Test server
166	NetWare management
26A	NetWare management
26B	Time synchronization
278	NetWare Directory server

add network service <service_name> status

- **server_type [server_type]**
- **socket [socket_number]**
- **enabled [YES]**
- **data [“string”]**

- **close_active_connections [TRUE | FALSE]**

This configures a network listener process that provides a certain type of service.

To see the available server types, use *list services*.

Parameter	Description
<service_name>	Name of this type of service. Limit of 32 character ASCII string.
server_type	Designates the type of server: **HTTP** **SNMPD** - SNMP agent **TFTPD** - server for file transfers **TELNETD** - TELNET server to the CLI
socket	Indicates which “socket” the server listens on. For TFTP and TELNET, it is the TCP or UDP port #.
enabled	This indicates whether the network service is enabled. Enter **YES** or **NO**.
data	Ancillary Data. This field contains server-specific configuration data. See the table on the next page for settable ancillary data parameters for TELNET.
close_active_ connections	Indicates whether or not to close any active connections when a service is disabled by the *disable network_service* command. Default: **FALSE**.

The table below shows configurable parameters for TELNET services, which are specified with the data parameter.

Ancillary Data Parameter	Description
auth	*On* indicates that login/password authentication should be performed on incoming connections. Default: **on**. Format: auth=[on/off]
login_prompt	ASCII string specifying the login prompt to be sent during authentication. It must be quoted. Default: “***login**: ”* Format: *login_prompt=[string]*
login_banner	ASCII string sent to a client when the connection is made. It must be quoted. Default: none. Format: *login_banner=[string]*

Add network service example

To configure a TELNET service to offer CLI access on port 23, doing authentication upon connect:

add network_service CLI_access server_type TELNETD socket 23

add snmp community <community_name>

- **address [ip_address]**
- **access [RO | RW]**

Adds to the list of SNMP authorized users. The community name and IP address of SNMP requests from managers on the network must match the list, which you can see using *list snmp communities*.

Parameter	Description
<community_name>	Group name that authorizes SNMP requests.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn
access	Determines what type of access to SNMP MIBs the added user will have. Options: Read Only (RO) and Read Write (RW).

add snmp trap_community <name>

- **address [ip_address]**

Adds to the list of community name/IP address pairs that are allowed to receive SNMP traps. You can see the list of authorized users with the *list snmp communities* command.

Parameter	Description
<name>	Group name defining who can receive SNMP traps.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn

add syslog <ip_name_or_addr> loglevel [loglevel]

Adds an IP host to the list of IP hosts that will receive syslog entries. You can see the current log levels for the system using *list facilities*, and modify the current log level for each facility using *set facility loglevel*.

Parameter	Description
<ip_name_or_address>	Host name or IP address of the Unix host that will receive syslog information.
loglevel	There are five levels of logging: **CRITICAL** - a serious system error, which may effect system integrity **UNUSUAL** - an abnormal event, which the system should be able to recover from **COMMON** - a regularly occurring event that is not frequent **VERBOSE** - a regular periodic event, e.g. a routing update message **DEBUG** - for debugging only

add tftp client <ip_name_or_addr>

Adds the tftp client to the authorization table for tftp access.

Parameter	Description
<ip_ name_or_addr>	Host name or IP address of a host to be added. An address of 0.0.0.0 allows all clients TFTP access.

add tunnel <tunnel_ name>

- **server_end_point [host name or ip_address]**

Sets up a VPN tunnel with the default values.

Parameter	Description
<tunnel name>	The name specified for the tunnel you are adding.
server_end_point	The host name or IP address of the VPN server at which this tunnel terminates.

add user [name] password [password]

- **{enabled [yes]}**

Adds a Telnet user to the local user table. The *list users* command displays these parameters for all users.

Parameter	Description
Name	Name of the user to be added, up to 32 ASCII characters.
Password	User’s password, up to 15 ASCII characters.
Enabled	This indicates whether the user is enabled. Enter **YES** or **NO**.

add vc [name]

Creates a virtual channel (VC) profile. Each profile represents a connection to a remote site. The *list vc* command displays a list of all configured VCs and their status. Use the *set vc* command to modify VC parameters.

When a VC profile is created, all of the different configurable parameters associated with the profile assume default values. The default values are specified in the VC profile named 'default'. You can display the current default values with the command *show vc default*.

Parameter	Description
name	Name of the user to be added, up to 32 ASCII characters.

ARP

arp <ip_name_or_addr>

- **output [outputfile_name]**

Prints the IP address (and Media Access Control Address [MAC] if on a locally connected network) of a network node to a file or the CLI (default). If a node is not in the ARP cache, an ARP request will be sent out.

Parameter	Description
<ip_name_or_addr>	IP address or node name for the IP and MAC address you seek.

DELETE

Delete commands remove anything you previously *add*ed.

delete access <ip subnet address>

The access list defines which Remote IP Subnets are allowed to access the Management services of the OCR812. Use this command to remove an entry in the list.

Parameter	Description
<ip subnet address>	IP address in the format xx.xx.xx.xx.

delete bridge network <network_name>

Deletes the previously *add*ed bridge network. Make sure you have disabled the bridge network, using the *disable bridge network* command, before trying to delete it. Use *list bridge forwarding* to see if there is any activity over the bridge connection.

delete configuration

Deletes all your configuration files, reboots the system and restores system configuration to default values.

delete dns host <host_name>

Deletes the specified host from the DNS Local Host Table. Use *list DNS hosts* to view the DNS Local Host table. After deletion, requests for that host will be processed through a DNS server, instead of locally. Use *list DNS servers* to see which servers are defined.

delete dns server <domain_name>

Removes the name server addresses associated with the specified domain from the Domain Name Server Table.

delete filter <filter_name>

Removes the named filter from the filter table, and deletes the file stored in FLASH memory. Use *list filters* to see what filter files are in FLASH memory.

delete file <file_name>

Deletes a file from the FLASH file system. Use *list files* to see which files are currently stored.

delete framed route vc

Deletes a framed route from the virtual channel profile.

delete ip network <network_name>

Deletes an IP network from the interface that you specified when *add*ing the network. Use *list ip networks* to see which networks are associated with which interfaces. Always use *disable ip network* before deleting it.

delete ip route <ip_address>

Deletes an IP address from the IP routing table, that you previously added with *add ip route*. Deleting this route will cause IP packets destined for this network to use the default route, which you can see using *list ip routes*. See *add defaultroute gateway* to find out how to add a default route.

delete ipx network <name>

Deletes an IPX network on the interface you specified with the add ipx network command. You can *list ipx networks* to see which are available, and the network's status. Be sure to use the *disable ipx network* command before deleting the network.

delete ipx route <ipx_net_address>

Deletes an IPX route on the interface you specified with the *add ipx route* command. The *list ipx routes* command displays the current IPX routes.

delete ipx service <service_name>

- **type [service_type]**

Deletes a static IPX service from the IPX services table. This command will work only if a complete match on all parameters is found. Refer to *add ipx service* command for more information.

Parameter	Description
service name	Designation of IPX service.
type	Type of service: file/server, print, etc.

delete pat tcp vc <vc_name>

- **public_port [number]**

delete pat udp vc <vc_name>

- **public_port [number]**

delete nat [dynamic | static] vc <vc name> public_pool_start <address>

- **public_address <ip_address>**

Deletes the static NAT mapping to this public IP address for the associated VC.

Parameter	Description
<vc_name>	The name of the vc for which you are deleting the static NAT mapping.
public_address	The public IP address of the static NAT mapping you wish to delete.

- **public_pool_start <ip_address>**

Deletes the dynamic NAT mapping to this pool of public IP address for the associated VC.

Parameter	Description
<vc_name>	The name of the vc for which you are deleting the dynamic NAT mapping.
public_address	The public IP pool start address of the dynamic NAT mapping you wish to delete.

delete network service <service_name> Deletes the specified network service from the list of available services. You must use *disable network service* before deleting the service. You can see which services are available and active using *list available services* and *list services*.

delete snmp community <name> Deletes an SNMP community that was previously added with the *add snmp community* command. You can use *list snmp communities* to see the current entries.

delete snmp trap_community <name> Deletes an SNMP trap community name from the list of names and IP addresses that are allowed to receive SNMP trap commands. You can use *list snmp communities* to see the current entries.

delete syslog <ip_name_or_address> Deletes the specified IP host name or IP address from the list of addresses which are authorized to receive syslog information. Use *list syslog* to see the currently allowed addresses.

delete tftp client <ip_name_or_address> Deletes the specified IP host name or IP address from the list of addresses which are authorized to TFTP. Use *list tftp clients* to see the currently allowed addresses.

delete tunnel <tunnel_name> Deletes the specified tunnel.

delete user <name> Deletes a user you previously added to the local user table. Use *list users* to see the currently defined user, and *show user* to see the attributes you assigned to that user using the *add user* or *set user* command.

delete vc <name> Deletes a virtual channel profile. Use *list vc* to see the currently defined VCs, and *show vc* to see the attributes of a specific VC. A VC must be disabled before it can be deleted.

DIAL

dial <vc_name> Generates an outgoing connection to the location specified by the vc name. You can use *list vcs* to list the defined vc profiles, and their current status.

DISABLE

disable access Disables the Access List feature. When disabled, all hosts are permitted to access the Router's management services.

disable bridge network <name> Disables the bridge network you previously defined using the *add bridge network* command. You can see which bridge networks are currently running using *list bridge forwarding*.

disable bridge spanning_tree Disables use of the spanning tree algorithm on bridge networks. The spanning tree algorithm is required if there is more than one bridge between the same two LAN segments. You can use *list bridge forwarding* to see which bridges are defined, and *show bridge network settings* to see which options are enabled on a particular bridge network.

disable command password Disables the console password feature.

disable icmp Disables the Internet Control Message Protocol.

disable interface <interface_name> Disables the specified interface. A disabled interface remains in the interface table, but will not transmit or receive any data. Use *list interfaces* to see the currently defined interfaces, and their status.

disable ip forwarding Causes the system to stop forwarding any packets over IP networks.

disable ip network <network_name> Disables the specified IP network. Make sure there is no activity on this network before disabling it.

disable ip rip Disables the RIP routing algorithm on all IP networks. You can use *show ip routing* to see the current status of IP routing. This saves system space by preventing a large RIP database, which is useful for networks connecting over the WAN interface.

disable ip routing Disables all routing protocols on all IP networks. Currently, the only routing protocol is RIP, which means that *disable ip rip* performs the same function. Use *show ip routing* to see the current status of IP routing.

disable ip static_remote_routes Disables all statically defined remote routes on all IP networks, that you previously defined using *add ip route*. You can list the current IP routes using *list ip routes*.

disable ipx network <network_name> Disables the specified IPX network. Use *list ipx networks* to see which IPX networks are defined, and their current status.

disable lan access

When the access list is enabled, this command disables access to Hosts on the local LAN interface. When disabled, all frames received on the LAN interface are subject to the access list check. If the corresponding LAN subnet is not in the access list, the frame is silently discarded.

disable link_traps interface <interface_name>

Prevents SNMP from sending linkup and linkdown traps for the specified interface. You can see if the interface is currently enabled for traps by using the *show interface settings* command.

disable network service <service_name>

Disables a network service, such as TELNET or TFTP. If *close_active_connection'* was specified as *TRUE* in the *add network_service* command, then all active connections will be closed when the server is disabled.

disable security_option snmp user_access

Turns off SNMP access to the CLI. This prevents remote users from using SNMP and possibly damage the configuration. You can use *enable security_option snmp user_access* to re-enable full SNMP access.

disable security_option remote_user administration

Disables CLI access to remote TELNET users. All CLI configuration must be done from the console port. You can use *enable security_option remote_user administration* to re-enable remote CLI access.

disable snmp authentication traps

Instructs SNMP to stop recording trap information for user (either local or remote) authentication.

disable telnet escape

Disables the TELNET escape character for all TELNET clients. When disabled, TELNET clients who press the escape character during their session will not get a local TELNET command line.

disable tunnel <tunnel_name>

Deactivates the specified tunnel.

disable user <user_name>

Disables the specified user from being used. It also causes all active sessions established using that particular user to terminate, and does not allow any new sessions to occur using that user name. Disabling a user is useful when prohibiting a user's access temporarily.

disable vc <user_name>

Disables the specified virtual channel from being used. It also causes any active session established using that particular VC to terminate, and does not allow any new sessions to occur using that VC. Disabling a VC is useful when prohibiting a VC's access temporarily.

DO

do <command_inputfile> output [outputfile]

Runs a script file that is stored in FLASH memory, which contains a series of CLI commands.

ENABLE

enable access Enables the Access List feature. When enables, only Remote Hosts in the access list are permitted access to the Router's management services.

enable bridge network <network_name> Enables bridging over the specified network. You must have previously run *add bridge network* to add bridging over this network. bridge networking is enabled by default, so you will only need to use this command if you have previously disabled this bridge. Note that bridging will not occur for a protocol, if routing is enabled for that protocol.

enable bridge spanning_tree Enables the spanning tree algorithm for the bridge connection. The spanning tree algorithm is required if there is more than one bridge between the same two LAN segments. You can use *list bridge forwarding* to see which bridges are defined, and *show bridge network <network_name> settings* to see which options are enabled on a particular bridge network.

enable command password <password> Enables the console password feature. When enabled, the user must login with the specified password before using the console port. This password is not the same password specified for Remote Login access. Once enabled, the unit must be sent back to the factory if the password is forgotten.

enable interface <interface_name> Enables the specified interface. Enabling an interface enables it to transmit and receive data. You can use *list interfaces* to see which interfaces are defined, and whether they are currently disabled.

enable ip forwarding Enables all IP networks to forward (route) packets. You should only need to use this command if you previously used *disable ip forwarding.*

enable ip network <network_name> Enables the specified IP network, which you previously defined using *add ip network*. You can use *list ip networks* to see the currently defined IP networks, as well as their current status.

enable ip rip Enables the RIP protocol for all IP networks. RIP protocol is set to NONE by default. You can check the RIP version using *show ip network settings*, and modify it using *set ip network.* RIP is enabled by default.

enable ip routing Enables all routing protocols for all IP networks. Currently, the only IP routing protocol this command enables is RIP, so it is functionally the same as *enable ip rip*.

enable ipx network <network_name> Enables the specified IPX network, which you previously defined using the *add ipx network* command. You can list currently defined IPX networks using *list ipx networks*.

enable lan access When the access list feature is enabled, this command enables access to all hosts on the local LAN interface. When enabled, all frames received on the LAN interface bypass the access list check.

enable link_traps interface <interface_name>

This command tells SNMP to send linkup and linkdown traps for the specified interface. You can see if the interface is currently enabled for traps using the *show interface settings* command.

enable network service <service _name>

Enables the network service that you previously defined with the *add network service* command. You can see which services are currently defined and their state using *list network services*.

enable security_option remote_user administration

Enables CLI access to remote TELNET and dial-in users. This prevents remote users from modifying the configuration. CLI configuration can be done from the console port and remote users. You can use *disable security_option remote_user administration* to restrict CLI access to the console port only and *enable security_option remote_user administration* to re-open full TELNET access.

enable security_option snmp user_access

Enables SNMP access to the user table. This allows remote users to use SNMP to update the user table, and gain unauthorized access to the CLI. Use *show security_options* to see the current security values.

enable snmp authentication traps

This command tells SNMP to send traps for both local and remote authentication. You can use *show snmp* to see the current setting.

enable tunnel <tunnel_name>

Enables the specified tunnel.

enable telnet escape

If the TELNET escape character was disabled by the *disable TELNET escape* command, this command re-enables it. When enabled, TELNET client users who press the TELNET escape key during their session will get a TELNET command line.

By default the escape character is control-]. A TELNET user can change it using *set escape* in the TELNET program.

enable user <user name>

Enables a user to establish TELNET sessions for remote management. You must have previously added the user using the *add user* command, where enabled is the default. The *list users* command displays a summary of all configured user profiles.

enable vc <vc name>

Enables a virtual channel to establish data sessions over the WAN. You must have previously added the VC using the *add vc* command, where disabled is the default. The *list vc* command displays a summary of all configured VC profiles.

exit CLI

If CLI password protection is enabled, this command forces an immediate logout from the CLI. The CLI password must be entered in order to access the CLI again.

HANGUP

hangup interface <interface_name>

Causes the connection on the specified interface to hangup (drop).

hangup vc <vc_name> Causes the connection for the specified VC to drop. You can see which VCs have active connections using *list vcs*. Also see *disable vc*, which causes a VC's session to drop, and prevents new sessions which use that VC from being established.

HELP

help <command> Provides information about possible commands and their formats. Typing help alone lists the possible commands. Typing help <command name> lists the possible parameters for that command.

Typing part of a keyword (command or parameter) and pressing Esc completes the keyword. If you have not yet entered enough of the keyword to be unique, pressing Esc causes the bell to ring.

Typing **?** after a command string displays the possible keywords and values for that command.

HISTORY

history Displays your previous CLI commands. You can recall commands from the history using ^P (C-P) to recall commands up the list, and ^N (C-N) to recall commands working down the list. The default depth is 10 commands. You can modify the history depth using the *set command history* command.

KILL

kill <"process name"> Kills an active process. Use *list processes* to see which processes are currently active. You can only *kill* a process that you started. An example would be a *ping* that you started that you now wish to kill.

LIST

list access Displays all IP Subnet addresses in the access list.

list active interfaces Displays the index, name, operational status, and administration status of all active interfaces. The output is the same as the *list interfaces* command, except non-active interfaces are not displayed. Inactive interfaces are interfaces with no current connections.

list bridge forwarding Displays the forwarding and filtering information

- **MAC address** - A unicast MAC address for which the bridge has forwarding and/or filtering data
- **Status** - One of the following:

  other - not one of the following

  invalid - aged out

  learned - learned, and in use

  self - statically defined, and in use

mgmt - unknown, but filtering information exists

- **RxPkt** - Number of packets received from this MAC station
- **RxOctets** - No. of bytes (octets) received from this MAC station
- **Fltr** - Number of packets received from this MAC station that were filtered out (discarded)
- **Fwd** - Number of packets received from this MAC station that were forwarded
- **TxPkt** - Number of packets forwarded to this MAC station
- **TxOctets** - Number of bytes forwarded to this MAC station

list call events Displays the last *twenty* call events. This is useful when trying to determine why a call over the WAN is not being established. The table displays the system, the up time, and the event.

list call log Displays the current call status for all VCs for which a call has been attempted. Each entry will include the VC name, the current call state (Disconnected, Connecting, or Connected), and the reason why the last call was cleared. Reasons for clearing include: line down, PPP timeout, Authentication error, Network configuration error, and termination initiated from either the local or remote side.

list critical events Displays the last *ten* critical status events, and the system time when each occurred. You can change which events are logged as critical, using the *set facility* command. The table displays the system, the up time, and the event.

list dns hosts Displays the DNS Local Host name and its IP address, which you configured using the *add dns host*.

list dns servers Displays DNS Name Servers, which you configured using the *add dns server* command. The domain name and the server address are listed for each DNS server.

list facilities Displays the system facilities (processes) currently running, plus the default log level. The log level is the severity of error that facility will produce syslog entries for. You can change the log level using the *set facility loglevel* command.

list filters Displays all the filter names in the filter table, which you previously defined using the *add filter* command. You can remove filters using *delete filter*. The command lists the filter file name, the status of the filter, and the protocols the file applies to. For example:

```
Filter Name     Status      Protocols
easyfilter.fil  NORMAL      IP IP-RIP
```

list files Displays the files currently stored in the FLASH file system. You can remove files using *delete file*, but you can add them using TFTP only.

list interfaces

Displays the installed interfaces, along with their operational status, administration status, and interface index. If an interface is down, you can use *enable interface* to try to bring it up. The command lists:

- **Index** - number used to identify the interfaces position in the table
- **Name** - interface name: *eth:1, DA:1* or *loopback*
- **Oper Status** - current, operating status of interface; UP or DOWN
- **Admin Status** - administrative status you designated interface to be, up or down. If it doesn't match Oper Status, a problem exists with the interface.

list ip addresses

Displays the IP address for each interface. It lists:

- **Address** - IP address of the interface
- **Bcast Algo** - broadcast algorithm used
- **Reassembly Max Size** - maximum allowable size of packet that can be reassembled from a fragmented packet
- **Interface** - interface this IP address uses to connect to the system

list ip arp

Displays the contents of the ARP cache. It lists:

- **IP Address** - IP address for this entry
- **Phys Address** - MAC address that the IP address maps to
- **Type** - interface type: Ethernet or Token Ring
- **If Name** - *eth:1, DA:1* or *loopback*

list ip interface_block

Displays the IP addresses associated with each system interface. If the interface has a point-to-point connection, then the neighbor field contains the address of the remote system. This command lists:

- **Address** - IP address of the interface
- **Neighbor** - IP address of the remote system
- **Status** - status of the connection; ENABLED or DISABLED
- **Interface** - *eth:1, DA:1* or *loopback*

list ip networks

Displays all the IP networks you previously defined using the *add ip network* command. It also lists:

- **Name** - network designation
- **Prot** - always the IP protocol
- **Int** - name of the interface this network runs on
- **State** - state of the network; ENABLED or DISABLED
- **Type** - STATIC or DYNAMIC network
- **Network Address** - address of the IP network

list ip routes

Displays all the statically defined IP routes that you previously defined using the *add ip route command*. It lists:

- **Destination** - IP address that the route resolves to

- **Prot** - LOCAL or RIP
- **NextHop** - address of the gateway used to reach this route
- **Metric** - number of router hops away this route is from the system
- **If** - interface that the route uses

list ipx networks Displays the IPX networks that you previously defined using the *add ipx network* command. It lists:

- **Name** - designation you assigned this network
- **Prot** - protocol; always IPX
- **Int** - interface each IPX network runs on
- **State** - ENABLED or DISABLED
- **Type** - STATIC or DYNAMIC
- **Network Address** - network address of this IPX network

list ipx routes Displays the IPX routes that you previously defined using the *add ipx route* command, plus the defined IPX nodes. It lists:

- **Network Addr** - network address of this route
- **Prot** - protocol used to find this route: LOCAL, RIP, STATIC, NLSP, OTHER
- **NextHopNIC** - network address of the next router (the next hop to the destination), or the MAC address for the local IPX nodes (on the LAN)
- **Gateway** - address of the gateway to this network
- **Metric Ticks** - number of hops through routers this network is distant from

list ipx services Displays IPX services. It lists:

- **Name** - name of the IPX service
- **NetNum** - network number that the service is on
- **Node** - name of the IPX node running the service
- **Socket Type** - socket number of the service
- **Prot** - protocol used to find this service: SAP, LOCAL, NLSP, STATIC or OTHER
- **Metric** - number of hops through routers to reach this service

list lan interfaces Displays the operational and administrative status (UP or DOWN), interface index number and name (eth:1) of all LAN interfaces. The output is the same as the *list interfaces* command, except only LAN interfaces are displayed.

list networks Displays all defined networks running any protocol. The command lists:

- **Name** - designation of the network that you defined with *add network*
- **Prot** - protocol of the network (IP or Bridging)
- **Int** - interface the network is running on
- **State** - ENABLED or DISABLED network

- **Type** - STATIC or DYNAMIC network
- **Network Address** - address of the network

list processes Displays all processes running on the system.

- **Index** - a reference number in the process table
- **Name** - designation of the process (e.g.: Domain Name System)
- **Type** - SYSTEM, APPLICATION, FORWARDER or DRIVER
- **Status** - ACTIVE, PENDING or INACTIVE

list ppp Displays PPP bundles and links. When multiple physical links are combined to run multilink PPP (RFC1717), the group of physical links is called a bundle. With the OCR 812, only a single link is supported.

This command displays:

- **Bundle Index** - index number of the physical interface in the bundle
- **Link Index** - index number in the list of links
- **Oper Status** - current operational status of the link
- **Interface Name** - designation of interface belonging to this bundle

list services Displays all network services you defined using the *add network service* command:

- **Name** - name of service
- **Server Type** - type of service. For example: tftp
- **Socket** - TCP port number used by the service
- **Close** - reveals whether all connections close when you disable this service: TRUE or FALSE. See *add network service* command for details.
- **Admin Status** - the status you have requested for this service: ENABLED or DISABLED. See the *add network service* command for details.

list snmp communities or **list snmp trap_communities** These commands display the defined SNMP communities, which you previously defined using the *add snmp community* command. *SNMP trap_communities* does not list access.

- **Community Name** - community designation for the IP address
- **IP address** - IP address of a member of the community
- **Access (Read/Write)** - type of access a member has to MIBs

list syslog Displays IP addresses which get syslog entries from the system. See *add syslog* for more information, and *delete syslog* command to remove entries. This command shows:

- **Syslog** - IP address to which syslog entries will be sent
- **Log Level** - reporting level of entries to send
- **Msg Count** - current number of messages sent since system bootup

Also see *list facilities* and *set facilities* commands, which let you view and change log reporting levels for each system facility.

list tcp connections Displays information about all TCP connections. Connection status is defined in RFC-793.

- **Local Address** - IP address of the local host for this connection
- **Local Port** - TCP port number used by the local connection
- **Remote Address** - IP address of the remote host for this connection
- **Remote Port** - TCP port number used by the remote connection
- **Status** - status of the connection. E.g.: *Listen*

list tftp clients Displays IP addresses of all users who allowed to use the Trivial File Transfer Protocol (TFTP) to connect to the system. You must have used *add network service* to add TFTP support to the system and used *add tftp client* to authorize users to connect.

list udp listeners Displays User Datagram Protocol (UDP) ports being used by the system. These ports correspond to processes which are receiving UDP data (for example SNMP, User Management, TFTP service). Local IP addresses and port numbers are listed for each UDP port.

list tunnel Lists (displays) the name and status of tunnels.

list users Lists all users, showing:

- **User Name** - user designation you specified using *add user*
- **Login Service** - The service used to login to the network (i.e. TELNET).
- **Status** - link status: ACTIVE, INACTIVE or DISABLED

list vc Lists all virtual channel profiles, showing:

- **Name** - user designation you specified using *add vc*
- **Network Service** - type of network service: RFC1483, PPP, PPPLLC
- **VPI** - Virtual Path Identifier
- **VCI** - Virtual Channel Identifier
- **Status** - link status: ACTIVE, INACTIVE or DISABLED

login_required Enables or disables CLI password protection.

password The CLI password. It must consist of 1 to 8 alphanumeric (printable) characters, inclusive.

PAUSED COMMANDS

More (or CR)	Continue printing
Quit	Cancel rest of output

PING

More (or CR) Continue printing

ping <ip_name_or_addr>

- **output [output_filename]**
- **count [count]**
- **interval [interval]**
- **timeout [timeout_value]**

Sends an ICMP echo request to a remote IP host. A reply from the pinged address indicates success.

Parameter	Description
<ip_name_or_address>	IP address in dotted notation, or host name of remote system.
output	A file name to direct output to.
count	Number of ICMP echo requests to send.
interval	Number of seconds to wait between sending each request.
timeout	Number of seconds to wait for an echo response to return.

QUICKVC

Runs the QuickVC Setup program to easily configure a virtual channel connection (remote site profile). See Chapter 5 for a complete description of the QuickVC Setup program.

REBOOT

Reboot the system. If you have made any configuration changes, be sure to *save all* before rebooting. Also see the *delete configuration* command.

RENAME

rename file <input_file> <output_file>

Renames files within the FLASH file system.

The FLASH file system is a flat file system (no subdirectories). Use the *list files* command to see what files currently exist.

Parameter	Description
<input_file>	Name of the original file.
<output_file>	New name for the file

RESOLVE

resolve name <ip_host_name>

Returns an IP Address for the specified host name by sending it to DNS for resolution. If the Domain Name has been specified using the *set DNS* command, it will also be resolved, otherwise you must specify it as part of the name. This command requires either a DNS local host entry (use *add DNS host*) or a DNS server (use *add DNS server*) to resolve the host name. It is the reverse of the *ARP* command.

SAVE

save all

Saves all changes you have made during your session with the CLI. It is a good idea to save your changes frequently, just as you should with any type of editor.

SET

set adsl reset

Resets the ADSL interface.

set adsl wire [pair]

Overrides the auto-direction of inner and outer pair wiring on the RJ-11 connector.

- **inner** - inner pair.
- **outer** - outer pair.

set bridge

- **aging_time <seconds>**
- **forward_delay <seconds>**
- **spanning_tree_priority <seconds>**

Sets parameters for all bridge networks.

Parameter	Description
aging_time	Interval to wait before aging out MAC addresses that were learned from other LAN segments. The default is 300.
forward_delay	Interval bridge waits before bridging packets. This time is useful for the bridge to listen to packets, look at the MAC addresses, and build its known MAC address table. Default is 15 seconds.
spanning_tree_ priority	Priority number determines who will be seen as the “root” bridge in a bridge network. The default is 32768.

set bridge firewall [firewall_mode]

Sets the mode of the Bridge Firewall function. The three modes are completely described in Chapter 6.

- **discard_routed_protocols** - packets for routed protocols are not bridged.
- **fwd_unicast_packets_only** - unicast packets for routed protocols may also be bridged. Broadcast and multicast packets are not bridged.
- **fwd_bc_and_unicast** - broadcast, multicast and unicast packets for routed protocols may also be bridged.

set command

- **history <numerical range>**
- **idle timeout <minutes>**
- **local_prompt <string>**
- **prompt <string>**

Sets console parameters for CLI commands.

Parameter	Description
history <numerical range>	Sets the depth of the buffer holding the command history. Use the *history* command to see the current depth and a list of your last CLI commands. The default is 10 commands. The range is 1-500.

prompt <string>	Sets the global command prompt for the CLI. Use *show command* to see the currently defined prompt. Limit: 64 characters.
local_prompt <string>	Sets a separate prompt for a command file process. Limit: 64 characters.

set date <date>

Sets the system date, and leaves the time unchanged. Use *show date* to see what the current settings are. The format is: dd-mmm-yyyy. The month should be the first three characters of the month name. The year can be either 2 or 4 digits (97 or 1997).

set dhcp mode <mode>

Sets the DHCP mode for the unit.

Parameter	Description
mode	DHCP functionality you wish to enable for this unit. Currently available services are: **DISABLED** - disables all DHCP services. **RELAY** - enables the DHCP Relay service. **SERVER** - enables the DHCP Server within the unit.

set dhcp relay server1

- **address <IP_address>**
- **enabled [YES | NO]**
- **max_hops <number>**

Defines the address and characteristics of the primary DHCP Server over the WAN that should receive our relayed DHCP requests.

Parameter	Description
address	IP address of the primary DHCP server over the WAN port where DHCP resolution requests should be forwarded.
enabled	Whether or not this server is active for relay.
max_hops	maximum number of hops the redirected requests are allowed to accrue without the request being dropped.

set dhcp relay server2

- **address <IP_address>**
- **enabled [YES | NO]**
- **max_hops <number>**

Defines the address and characteristics of the secondary DHCP Server over the WAN that should receive our relayed DHCP requests.

Parameter	Description
address	IP address of the secondary DHCP server over the WAN port where DHCP resolution requests should be forwarded.
enabled	Whether or not this server is active for relay.
max_hops	maximum number of hops the redirected requests are allowed to accrue without the request being dropped.

set dhcp server

- **DNS1 <IP_address>**
- **DNS2 <IP_address>**
- **domain <string>**
- **end_address <IP_address >**
- **hostname <string>**
- **lease <seconds>**
- **mask <IP_address>**
- **router <IP_address>**
- **start_address <IP_address>**
- **WINS1 <IP_address>**
- **WINS2 <IP_address>**

Defines the characteristics of the DHCP Server and defines the pool of addresses that this facility should administer.

Parameter	Description
DNS1	IP address of the primary DNS server that the DHCP server will utilize when resolving names.
DNS2	IP address of the secondary DNS server that the DHCP server will utilize when resolving names.
domain	Name of the DNS domain we exist in.
end_address	Last IP address in the pool of IP addresses that will be handed out through DHCP.
hostname	DNS hostname of this unit.
lease	The number of seconds that an IP address will be allocated to a workstation without having to be renewed.
mask	IP network mask that applies to the pool of IP addresses being administered.
router	IP address that the workstations should use as their default gateway.
start_address	First IP address in the pool of IP addresses that will be handed out through DHCP.
WINS1	IP address of the primary WINS server that the DHCP server will utilize.
WINS2	IP address of the secondary WINS server that the DHCP server will utilize.

set dns

- **cache_size <number>**
- **number_retries <number>**
- **timeout <seconds>**

Sets the global parameters for DNS; both the local DNS hosts (*list DNS host*) and the remote DNS servers (*list DNS servers*).

Parameter	Description
cache_size	Enter the size of the cache. The valid range is from 20-500.
number_retries	Number of times the resolve name request will be sent to each Name Server if the server fails to respond to a request before the timeout period. Default is 1, valid range is 1-5.

timeout	Number of seconds to wait before deciding a request to a Name Server has timed out. Minimum interval and default is 5 seconds, maximum interval is 120 seconds.

set facility <facility_name> loglevel [level]

Sets the severity reporting level for a facility. The hosts that will receive the error log entries are defined using *add syslog loglevel*. Use *list facilities* to see what the current loglevel is for each facility. The levels:

- **CRITICAL** - a serious system error, which may effect system integrity
- **UNUSUAL** - an abnormal event, which the system should recover from
- **COMMON** - a regularly occurring event that is not frequent
- **VERBOSE** - a regular periodic event, e.g. a routing update message
- **DEBUG** - for debugging purposes only

set ilmi vpi <number> vci <number>

This allows modification of the Virtual Path or Channel ID that will be used for exchanging ILMI (Integrated Local Management Interface) messages.

Parameter	Description
vpi	The virtual path identifier for the ILMI.
vci	The virtual channel identifier for the ILMI.

set interface <interface_name>

- **filter_access [ON | OFF]**
- **input_filter <filter_name>**
- **output_filter <filter_name>**

Sets filter parameters for the specified protocol on the specified interface. You can see the available filter files using *list filters*, view the contents of a filter file using *show filter*, and add filter files to FLASH memory using TFTP.

Parameter	Description
<interface_name>	Designation of interface you are setting parameters for. Limit of 32 characters.
filter_access	ON causes filters specified for an interface with a *set interface* command, to override filters specified with a *set user* command, when the filters are of the same type.
input_filter	Name of filter file you wish to be applied to the input stream coming in on the specified interface. Limit: 20 characters.
output_filter	Name of the filter file you wish to be applied to the output stream leaving the specified interface. Limit: 20 characters.

set ip network <name>

- **broadcast_algorithm [number]**
- **reassembly_maximum_size [number]**
- **rip_authentication [string]**
- **rip_policies_update <rip_policies>**
- **routing_protocol [NONE | RIPV1 | RIPV2]**

Sets the broadcast algorithm, the maximum size used for reassembling fragmenting packets, the RIP authentication string, RIP policies, and the routing protocol for the specified interface. The only required parameter for this command is <name>. All other parameters are optional. You can set all of them at once, or one at a time. This command can only be used on IP networks that have already been defined using *add ip network*. You can list the currently defined IP networks using *list ip networks*. You must also disable the network before setting these parameters, using *disable ip network*.

RIP Policies: The following RIP policies are supported by the IP route:

- **Send Default** - *disabled* by default, causes router to advertise itself as the default router.
- **Send Routes** - *enabled* by default. Tells RIP to advertise (broadcast) its routes on the network every 30 seconds - is standard for a gateway router.
- **Send Subnets** - *disabled* by default. If this flag is on, only routes having the same network mask and are subnets of the same network are sent out the interface.
- **Accept Default** - *disabled* by default. Determines whether router accepts default route advertisements.
- **Split Horizon** - *enabled* by default. Records the interface over which it received a particular route and does not propagate its information about that route back over the same interface. This prevents route broadcasts from looping between routers.
- **Poison Reverse** - *enabled* by default. Routes that were excluded due to the use of split horizon are instead *included* with infinite cost (16). The system continues to broadcast the route, but with an infinite cost. This policy speeds the news that a link is down to the rest of the internetwork's routers. In general, it performs better when used with split horizon.
- **Flash Update** - *enabled* by default. It is also known as "triggered update", meaning broken routes will be advertised immediately, instead of waiting for the next scheduled broadcast.

The following flags are for backward compatibility with RIP version 1 when RIP version 2 is selected as the routing protocol:

- **Send Compatibility** - Controls the selection of destination MAC and IP addresses. It is *enabled* by default. When enabled, *broadcast* address is used; when disabled, *multicast* address is used.
- **RIP V1 Receive** - Controls the receipt of RIP version 1 updates. When RIP version 1 is the selected routing protocol, this policy is *enabled* by default, which means RIP version 1 packets are received. (When RIP version 2 is chosen, this policy is en*abled* by default, meaning RIP version 1 packets are received.
- **RIP V2 Receive** - Controls the receipt of RIP version 2 updates. When RIP version 1 is the selected routing protocol, this policy is *enabled* by default, which allows RIPV1 packets to be received. When RIP version 2 is selected, this policy is *enabled* by default, allowing RIPV2 packets to be received.
- **Silent** - This flag tells RIPv2 not to send updates. It is *disabled* by default.

Parameter	Description
<network_name>	Designation of the IP network for which you want to set parameters.
broadcast_algorithm	Algorithm determines which address is used in broadcasts to represent the entire network. Choices are: **1** - the IETF standard, nnn.nnn.nnn.255 (default) **0** - the BSD standard, nnn.nnn.nnn.000
reassembly_ maximum_size	Maximum size IP datagram that the system will try to reassemble, when the datagram has been fragmented to fit in the network packet size. The default is 3468.
rip_authentication	Text string used for RIPv2 authentication.
rip_policies_update	Allows user to enable or disable RIP policies. See text on the preceding page for description of keywords. A keyword with a NO_ in front is used to disable the policy. The default is indicated by **(D)**. SEND_DEFAULT/NO_SEND_DEFAULT**(D)** SEND_ROUTES**(D)**/NO_SEND_ROUTES SEND_SUBNETS/NO_SEND_SUBNETS**(D)** ACCEPT_DEFAULT/NO_ACCEPT_ DEFAULT**(D)** SPLIT_HORIZON**(D)**/NO_SPLIT_HORIZON POISON_REVERSE**(D)**/NO_POISON_ REVERSE FLASH_UPDATE**(D)**/NO_FLASH_UPDATE SEND_COMPAT**(D)/**NO_SEND_COMPAT RIPV1_RECEIVE**(D)**/NO_RIPV1_RECEIVE RIPV2_RECEIVE**(D)**/NO_RIPV2_RECEIVE SILENT **(default is disabled)**
routing_protocol	Sets routing protocol to be used on IP network. Choices are: no routing protocol, RIP version 1, or RIP version 2.

set ip routing

- **autonomous_system_number [number]**
- **table_maximum_size [number]**
- **metric_maximum_entries [number]**
- **rip_flags [METRICS, SEND_REQUEST]**
- **router_id [router_id]**

Sets parameters for IP routing to the specified IP router address, which is the gateway to an Autonomous System.

Parameter	Description
autonomous_system_number	Autonomous system number.
table_maximum_size	Maximum number of IP routes system can hold in its table. Default: 1000
metric_maximum_entries	Most next hop entries the system table can maintain.

rip_flags	Flags indicate at which level a RIP instance is disabled or configured. Choices are: **METRICS** - Specifies how to increment metrics using RFC1058. **SEND_REQUEST** - Sends a RIP request for routing information when an interface first comes up.
Router_id	The IP station address of the ip router.

set ipx network <network_name>

- **delay_ticks [number]**
- **diagnostics [DISABLE | ENABLE]**
- **maximum_learning_retries [number]**
- **netbios [ENABLE | DISABLE]**
- **netbios_name_cache [DISABLE | ENABLE]**
- **netbios_cache_timer [seconds]**
- **netbios_max_hops [number]**
- **packet_maximum_size [number]**
- **rip [BOTH | DISABLE | LISTEN | RESPOND_ONLY | SEND]**
- **rip_age_multiplier [number]**
- **rip_packet_size [number]**
- **rip_update_interval [number]**
- **sap [BOTH | DISABLE | LISTEN | RESPOND_ONLY | SEND]**
- **sap_age_multiplier [number]**
- **sap_packet_size [number]**
- **sap_nearest_replies [ON | OFF]**
- **sap_update_interval [number]**

Sets parameters for the specified IPX network.

Parameter	Description
<network_name>	Designation of the IPX network. Maximum size is 32 characters.
delay_ticks	Interval in number of ticks it takes to reach this IPX network.
diagnostics	Whether or not to send diagnostic packets to this IPX network.
maximum_learning_ retries	Number of times this network will re-send packets to learn its directly connected neighbors.
netbios	Whether to support NetBIOS on dial-out IPX networks.
netbios_name_cache	Whether or not to cache a list of the other NetBIOS systems on this IPX network.
netbios_cache_timer	How long a NetBIOS system will be kept in the cache.
netbios_max_hops	Maximum number of hops this network will make to locate a NetBIOS system.

packet_maximum_size	Maximum size packet that this IPX network will support.
rip	Sets the RIP mode.
rip_age_multiplier	Number to multiply the rip_update_interval by, to obtain the value for the aging out the entries in the RIP database.
rip_packet_size	Size of RIP packets.
rip_update_interval	How often RIP should send periodic updates.
sap	Sets the SAP mode.
sap_age_multiplier	Number to multiply the sap_update_interval by, to obtain the value for aging out entries in the SAP database.
sap_packet_size	Size of SAP packets.
sap_nearest_replies	Whether or not SAP will look its nearest neighbors.
sap_update_interval	How often RIP should send periodic updates.

set ipx system

- **priority [priority level]**
- **default_gateway [ipx_host_add]**
- **initial_pool_address [ipx_addr]**
- **pool_members [number]**

Sets parameters for dynamic IPX networks.

Parameter	Description
priority	Priority for the dynamic IPX network.
default_gateway	Default router for the dynamic IPX network.
initial_pool_address	Initial IPX address used to dynamically assign IPX network.
pool_members	Number of addresses to reserve in the pool of IPX addresses used when dynamically assigning IPX networks.

set network service <admin_name>

- **server_type [server_type]**
- **socket [socket_number]**
- **data [“string”]**
- **close_active_connections [TRUE | FALSE]**

Sets parameters for configured network services.

You can list the configured network services using *list network services*. The service must be disabled for this command to work.

Parameter	Description
<admin_name>	Designation you assigned to network service with the *add network service* command. Limit of 32 characters.

server_type	Type of network service you wish to assign to this administration name. Currently available services are: **TELNETD** - TELNET server **HTML** - for gathering statistics **SNMPD** - SNMP agent **TFTPD** - server for file transfers
socket	Indicates which "socket" the server listens on. For TFTP and TELNET, it is the TCP or UDP port number.
data	TELNET Ancillary Data. This field contains server-specific configuration data. See table which lists the configurable *ancillary data* parameters.
close_active_connections	Indicates whether or not to close any active connections when a service is disabled by the *disable network_service* command.

set ppp receive_authentication [ANY | ANY_EXCEPT_MSCHAP | CHAP | MSCHAPV1 | MSCHAPV2 | NONE | PAP]

Sets the type of inbound authentication to be used when establishing PPP connections for PPTP and L2TP tunnels.

For in-depth information about CHAP and PAP, see RFC 1334.

*A VPN tunnel can **only** be configured for MSCHAPv1 by using the CLI **set ppp** command (MSCHAPv1 **cannot** be configured via the OCR 812 web interface).*

*To use PPTP with CHAP for a VPN established between the OCR 812 and a Windows 2000 Server, you must ensure that **store pw using reversible encryption for all users in domain** is set to enabled **before** adding VPN users. For more information, see **Configuring Windows 2000 Server to Support CHAP Authentication**.*

Authentication Options

Parameter	Description
ANY	The default. Use whatever type of authentication is requested.
ANY_EXCEPT_MSCHAP	Use any type of authentication *except* Microsoft Challenge Handshake Authorization Protocol version 1.
CHAP	Use Challenge Handshake Authorization Protocol.
MSCHAPv1	Use Microsoft Challenge Handshake Authorization Protocol version 1. Note that you must enter the **set tunnel** command at the CLI prompt and specify both a user name and a password.
MSCHAPv2	Use Microsoft Challenge Handshake Authorization Protocol version 2. Note that you must enter the **set tunnel** command at the CLI prompt and specify both a user name and a password.
NONE	Don't check for authentication.
PAP	Use Password Authentication Protocol.

set tunnel <tunnel_ name>encryption_algorithm [AUTO | MICROSOFT_128BIT | MICROSOFT_40BIT | MICROSOFT_56BIT | NONE | REQUIRED]

Sets encryption for a PPTP or L2TP tunnel.

Encryption can be set to any of the parameters shown in the Table below. **However**, a tunnel can only be configured for Microsoft 40-bit, 56-bit, and 128-bit encryption (MPPE) if the **MSCHAPv1** authentication protocol is set to enabled. To enable MSCHAPv1, enter the *set ppp receive_authentication* command and specify the MSCHAPv1 option.

*The OCR 812 implementation of MPPE (Microsoft Point-to-Point Encryption) will not work if MSCHAPv**2** authentication is **required** by the server (to use MPPE, you must set your system to use MSCHAPv**1**).*

*If you must authenticate with MSCHAPv2, we suggest you set encryption to **NONE** (otherwise, it may be impossible to connect to sites that require MSCHAPv2 authentication).*

MPPE Options:

Parameter	Description
AUTO	Use whatever type of encryption is requested.
MICROSOFT_128BIT	Use the strongest level of MPPE encryption.
MICROSOFT_40BIT	Use the weakest level of MPPE encryption.
MICROSOFT_56BIT	Use the medium level of MPPE encryption.
NONE	Use no encryption. This is the **default** encryption setting.
REQUIRED	Some type of encryption is required. If at any time encryption is (or becomes) unavailable, the tunnel link is terminated.

*MPPE (Microsoft Point-to-Point Encryption protocol) does **not** support encryption for L2TP tunnels.*

set ppp echo_retries <number>

Sets the number of PPP echo request retries that will be attempted before declaring a PPP link down. When set to a non-zero value, PPP echo requests will periodically be sent on all active PPP links. If a <number> consecutive PPP echo responses are not received, the PPP link will be declared down. The maximum <number> of PPP echo retries is 10. When set to 0 (the default), no PPP echo requests will be sent - the feature is disabled.

set snmp community <community_name>

- **address [IP_address]**
- **access [RO | RW]**

Modifies parameters for an SNMP authorized user. The community name and IP address of SNMP requests from managers on the network must match the list, which you can see using list snmp communities.

Parameter	Description
<community_name>	Group designation authorizing SNMP requests.
address	IP address of the SNMP manager, in the form nnn.nnn.nnn.nnn
access	Determines what type of access to SNMP MIBs the added user will have. Options are Read Only (RO) and Read Write (RW).

set system

- **name ["name"]**
- **location ["location"]**
- **contact ["contact info"]**
- **transmit_authentication_name [name]**

Specifies system contact information, which is displayed using *show system*. The user name is the remote account name. *Location*, *name* and *contact* names are limited to 64 characters.

Parameter	Description
name	A name identifying the user to the system.
location	The location of the user.
contact	The information contact for the user.
transmit_ authentication_name	Deprecated

set syslog <ip_address> loglevel [level]

Sets the error reporting level for syslog entries that will be sent to the specified IP address. You must have previously defined this syslog IP address using *add syslog*. There are ***five*** levels of logging:

- **CRITICAL** - a serious system error, which may effect system integrity
- **UNUSUAL** - an abnormal event, which the system should recover from
- **COMMON** - a regularly occurring event that is not frequent
- **VERBOSE** - a regular periodic event, e.g. a routing update message
- **DEBUG** - for debugging only

set time <time>

Sets the system time, and leaves the date unchanged. Use *show date* to see what the current settings are. The format is: hh:mm:ss. The seconds field is optional.

set tunnel <tunnel_name>

Modifies tunnel parameters.

The following is a list of *set tunnel* parameters and supported values:

Table 6-7 812 Set Tunnel Parameters and Supported Values

Parameter	Supported Value	Remarks
ENCRYPTION_ALGORYTHM	NONE	
MTU	1400	
TUNNEL_TYPE	PPTP, L2TP	PPTP is the default.
INPUT_FILTER	<filter_name>	
OUTPUT_FILTER	<filter_name>	
PASSWORD	<password>	

Table 6-7 812 Set Tunnel Parameters and Supported Values

Parameter	Supported Value	Remarks
SEND_PASSWORD	<password>	The SEND_PASSWORD must match the authentication password on the VPN server. You must change the default SEND_PASSWORD using the **SET TUNNEL** command.
ENCRYPTION_ALGORITHM	NONE AUTO MICROSOFT_128BIT MICROSOFT_40BIT MICROSOFT_56BIT REQUIRED	
MTU	1400	
SEND_NAME	<name>	The SEND_NAME must correspond with the authentication name on the VPN server. If you do not specify <name>, the system sets the value for this field to <tunnel name>.
NAT_OPTION	PAT	
LOCAL_IP_ADDRESS	<ip_address>	255.255.255.255 is the recommended setting for LOCAL_IP_ADDRESS
REMOTE_IP_ADDRESS	<ip_address>	255.255.255.255 is the recommended setting for REMOTE_IP_ADDRESS

set user <user_name>

- **message [“message”]**
- **password [password]**
- **session_timeout [seconds]**
- **tcp_port [tcp_port]**
- **terminal_type**

Modifies user parameters.

Parameter	Description
<user_name>	Name of user, previously defined using *add user*. Limit of 32 characters.
message	Message presented to a dial-in user.
password	User’s password, up to 15 ASCII characters. Value is required.

session_timeout	Interval before timing out a session.
tcp_port	TCP Port number for the Telnet session.
Terminal_type	The type of terminal. This is an alphanumeric string, of up to 64 characters.

set vc <vc_name>

- **address_selection [negotiate | assign | specified]**
- **bridging [enable | disable]**
- **default_route_option [enable | disable]**
- **destination_address [ip address]**
- **end_time [HH:MM:SS]**
- **header_compression [none | TCPIP]**
- **idle_timeout [seconds]**
- **input_filter [filter_name]**
- **ip [enable | disable]**
- **ip_routing [listen | send | both | none]**
- **ip_source_validation [enable | disable]**
- **ipx [enable | disable]**
- **ipx_address [ipx_addr]**
- **ipx_routing [all | listen | respond | send | none]**
- **ipx_wan [enabled | disabled]**
- **local_IP_address [ip_net_address]**
- **mac_routing [enable | disable]**
- **MTU [number]**
- **NAT_option [disable | enable | nat | pat | super_nat]**
- **PAT_default_address [ip_addr]**
- **network_service [ppp | PPPLLC | RFC_1483]**
- **output_filter [filter_name]**
- **password [password]**
- **remote_ip_address [ip_addr]**
- **rip [ripv1 | ripv2]**
- **rip_authentication [string]**
- **rip_policies_update [rip_policies]**
- **send_name [ ]**
- **send_password [“text string”]**
- **type [ONDEMAND | CONTINUOUS | MANUAL]**

Specifies parameters for VCs.

Parameter	Description
<vc_name>	VC profile name.
address_ selection	Determines how the IP address will be assigned for remote IP network connections. **NEGOTIATE** - learn the remote IP address. **SPECIFIED** - uses IP address set in remote_IP_address value
bridging	Enables/disables bridging across this link.
default_route_ option	When enabled, a default route is automatically created (by negotiation) with the remote router's IP address.
Destination_ address	For an SVC, this is the destination E.164 address to which a connection will be established.
End_time	This field is the end time for the virtual circuit. The expected format is HH:MM:SS. The Seconds field is optional.
Header_ compression	This determines whether you will have no compression on cell headers, or if you will use TCP/IP compression on the cell headers transmitted across this vc.
idle_timeout	Interval to wait before timing out an inactive connection. Default: 300 seconds.
input_filter	Designation of the filter file in FLASH memory to be applied to the input data stream.
ip	Sets interface to enable/disable protocol. Default is enable.
ip_routing	Sets routing type (RIP packets) accepted on this connection. Options: **LISTEN** - detects packets destined for system's nets **SEND** - routes packets destined for the remote network **BOTH** - both of the above **NONE** - ignores all routing packets
ip_source_ validation	When enabled, any packet who's source IP address falls within the LANs IP network will be dropped.
ipx	This controls whether to enable or disable IPX for the virtual circuit. The choices are [ENABLE, DISABLE].
ipx_address	This sets the IPX address for the virtual circuit.
ipx_routing	This sets the routing type (RIP packets) accepted on this connection. Options are: **ALL** - listens, sends, and responds RIP packets. **LISTEN** - detects packets destined for the system's network. **NONE** - ignores all routing packets. **RESPOND** - responds by sending out packets **SEND** - routes packets destined for the remote network.
ipx_wan	This determines if IPX is enabled or disabled for the WAN. Options are [ENABLED, DISABLED].
local_IP_address	IP address of the VC making an IP connection over the WAN interface. There are two special values which may be assigned to the local_IP_address: The local_IP_address should be learned via PPP negotiation (255.255.255.255). The interface is Unnumbered (0.0.0.0).
mac_routing	Determines if MAC-Encapsulated Routing is enabled.

management_ip_ address	Secondary IP address on the VC for Management purposes only. If the Management IP address is configured, the 'local_IP_address' must be configured as numbered. Address is configured with the following format: xx.xx.xx.xx/nn -- where *nn* is the number of bits in the netmask or netmask class (i.e., A, B, or C).
MTU	Maximum Transfer Unit - largest data packet size allowed.
NAT_option	Enable or disable PAT, NAT, or Super NAT.
PAT_default_ address	Default workstation address that incoming IP traffic will get forwarded to if the demuxing of the network address translation is unresolved.
Network_service	Type of network service. Default is PPP.
output_filter	Name of filter file in FLASH memory to be applied to output data stream.
Password	The password is an alphanumeric string of maximum size 15 characters.
remote_IP_address	For a client IP connection, address assigned to the client.
Rip	Selects either RIPV1 or RIPV2 for IP RIP.
rip_authentication	Text string used for RIPv2 authentication.
rip_policies _update	Allows VC to enable or disable RIP policies. See text on the preceding page for description of keywords. A keyword with a NO_ in front is used to disable the policy. Default is indicated by **(D)**. SEND_DEFAULT/NO_SEND_DEFAULT**(D)** SEND_ROUTES**(D)**/NO_SEND_ROUTES SEND_SUBNETS/NO_SEND_SUBNETS**(D)** ACCEPT_DEFAULT/NO_ACCEPT_ DEFAULT**(D)** SPLIT_HORIZON**(D)**/NO_SPLIT_HORIZON POISON_REVERSE**(D)**/NO_POISON_ REVERSE FLASH_UPDATE**(D)**/NO_FLASH_UPDATE SEND_COMPAT**(D)**/NO_SEND_COMPAT RIPV1_RECEIVE**(D)**/NO_RIPV1_RECEIVE RIPV2_RECEIVE**(D)**/NO_RIPV2_RECEIVE SILENT **(default is disabled)**
send_name	An identification name sent to the remote network.
send_password	Password sent to the remote network. Limit: 15 characters.
Type	Describes type of connection. Options: **ONDEMAND** - makes connection when the system needs a session with the remote network. **CONTINUOUS** - keeps connection up all the time **MANUAL** - manually starts connection using the CLI

set vc <vc_name> atm

- **set [number]**
- **category_of_service [Unspecified (UBR) | Variable (VBR)]**
- **pcr [number]**
- **scr [number]**
- **type [PVC | SVC]**
- **vci [number]**
- **vpi [number]**

Sets ATM parameters for VCs.

Parameter	Description
<vc_name>	VC profile name.
Bt	Burst Tolerance (VBR only).
Category_of_service	Select either Unspecified (UBR) or Variable (VBR).
Pcr	Peak Cell Rate (both UBR and VBR).
Scr	Sustained Cell Rate (VBR only).
Type	This designated a virtual circuit as either a Switched Virtual Circuit (SVC) or a Permanent Virtual Circuit (PVC).
Vci	Virtual Channel Identifier.
Vpi	Virtual Path Identifier.

SHOW

Show commands display details about system entities.

show access

Displays the current status of the access list feature.

- **Administration Status** - Indicates status of the access list feature. Options are *Enabled* or *Disabled*.
- **LAN Access** - Indicates whether all frames received on the LAN interface are subject to access list checking.
- **Number of Frames Blocked** - Number of frames silently discarded because the Remote Host's subnet was not on the access list.

show atm status

Displays current statistics for the ATM protocol running over the ADSL WAN interface. It lists:

- **Cell Delineation** - Whether or not cell delineation is currently achieved.
- **ILMI VPI** - ILMI Path Identifier used for obtaining dynamic VC's (Not supported in OfficeConnect Remote 812 1.0).
- **ILMI VCI** - ILMI Channel Identifier used for obtaining dynamic VC's (Not supported in OfficeConnect Remote 812 1.0).
- **TX Cells** - Number of ATM data cells sent over the WAN.
- **TX Idle Cells** - Number of ATM idle cells sent over the WAN.
- **RX Good Cells** - Number of well-formed and correctly addressed ATM data cells received from the WAN.
- **RX Idle Cells** - Number of well-formed and correctly addressed ATM idle cells received from the WAN.
- **RX No Pkt Avail** - Number of times a packet was reassembled but could not be delivered over the LAN because of lack of packet memory within the OCR 812.
- **RX Bad VPI or VCI** - Number of ATM cells received with a bad or inactive VPI and/or VCI number.
- **RX Bad HEC** - Number of ATM cells received with a bad ATM header.
- **RX Queue Full** - Number of times a packet was dropped because the RX queue was full.

show adsl statistics

Statistics for both near end and far end ADSL/ATM link. Counters include corrected frames, CRC errors, and HEC errors for the Fast and Interleaved path.

show adsl performance

Fields:

- **Number of link down events**
- **Total time since system reboot (hours, minutes, seconds)**
- **Total time since last linkdown:**
- **Errored seconds since last link down:**
- **Total errored seconds in 15 minutes:**
- **Total errored seconds in previous 15 minutes:**

show adsl transceiver_status

Displays the current status of the ADSL/ATM link.

Fields:

- **Operational Mode**: either "loss of signal" or "operational".
- **Attenuation Upstream**
- **Attenuation Downstream**
- **Noise Margin Upstream**
- **Noise Margin Downstream**
- **Transmit Power (ATUR)**
- **Transmit Power (ATUC)**
- **Actual Negotiated Downstream Baud Rate:**
- **Actual Negotiated Upstream Baud Rate:**

show adsl version

Fields:

- **ADSL hardware release version: 0x3530**
- **ADSL Alcatel chipset firmware release version: 141**

show bridge network <name>

- **counters** [Received Frames, Transmit Frames, Discarded]
- **settings** [Interface, Network Address, Frame Type, Status, User Name, Spanning Tree Enabled]

Parameter	Description
counters	Displays information about the specified bridge network. It lists: **Received Frames** - packet frames which have been received **Transmit Frames** - packet frames which have been sent **Discarded** - packet frames which have been thrown away

(continued)

settings	Displays information about the specified bridge network. You use *add bridge network* to define bridge networks. **Interface** - the interface this bridge is using **Network Address** - index number for this bridge network **Frame Type** - BRIDGE is the default **Status** - ENABLED or DISABLED are options **User Name** - user to supply parameters for this bridge **Spanning Tree Enabled** - ENABLED or DISABLED

show bridge settings

Displays the settings for all bridge networks. Use *set bridge* to modify these values.

- **Base Aging Time** - time to age out a known MAC address, default 300
- **Spanning Tree Forward Delay** - delay after coming up before learning, default is 15
- **Spanning Tree Priority** - this bridge's bid to be root bridge, default is 32768
- **Access MACs Only** - This can be enabled or disabled.
- **Spanning Tree Mode** - sets spanning tree algorithm on. Default is DISABLED
- **Base MAC Address** - address of the bridge
- **Number of Networks** - number of networks in this bridge
- **Type** - type of bridge: TRANSPARENT_ONLY is the default

show call_log

Displays the current call status of a specified VC.

Fields:

- **Call State:** current call state of the call (i.e. Disconnected, Connecting, Connected).
- **Last Clearing reason:** indicates why the call was cleared. Reasons for clearing include, line down, PPP timeout, Authentication error, Network configuration error, and termination initiated from the local and remote side.
- **IP, IPX, and Bridge status:** current status of each network layer.
  - **Configured -** protocol is configured for this VC and the call is being initiated
  - **Not configured -** The protocol is disabled on this VC.
  - **Established -** Protocol was negotiated successfully and is currently active on this VC.
  - **Failure -** Protocol was configured, but there was a failure in the PPP negotiation while attempting to initiate the network layer.

show command

Displays the settings for Command History Depth, and the Current Prompt. You can modify the history depth using *set command history*, and alter the prompt using *set command prompt*. Prompts can hold a maximum of 64 characters. For example:

History Depth:	**10**
Current Prompt:	**OCR-DSL>**
Local Prompt:	**OCR-DSL>**

show configuration Displays a variety of system information including: System Identification, Authentication Remote, Remote Accounting, Interfaces, IP forwarding, IPX Default Gateway, Bridge Spanning Tree, and DNS Domain.

show critical_event settings Displays where the log files for critical event messages are stored in the FLASH file system.

- **Critical Event Sink** - where critical events are logged, default is @file:/./log-file.local
- **Critical Event Backup** - where critical events are logged, if the first destination fails, default is @file:/./old-log-file.local

show date Displays the system *date, time,* and *uptime*. For example:

```
System Date:            09-FEB-2107 15:06:10
System UpTime:          2d 08:37:54
```

show dhcp client <vc name> status Displays the current DHCP Client status for the specified VC. If multiple VCs are configured with DHCP enabled, each VC will have a unique DHCP Client status.

- States:

  Discovering - The DHCP Client is broadcasting Discover messages, waiting for an Offer response from the Server.

  Requesting - The DHCP Client is requesting an IP address and waiting for an ACK response from the Server.

  Established - The DHCP Client has successfully been assigned an IP configuration from the Server.

- IP configuration learned/assigned by the DHCP Server:

  IP Address
  IP Mask
  Gateway Address
  Primary DNS Address
  Secondary DNS Address
  Lease Time

- Statistics:

  Number of Discovers transmitted
  Number of Requests transmitted
  Number of Declines transmitted
  Number of Offers received
  Number of ACKs received
  Number of NACKs received
  Number of errors detected

show dhcp relay

Displays the current configuration and counters for both the primary and secondary DHCP relay server.

- **IP Address** - IP address of the DHCP Server.
- **Max Hops** - maximum hops to get to this server.
- **Status** - enabled or disabled.
- **Request Sent to Server** - number of requests sent to server.
- **Responses Received from Server** - number of responses received from the server.
- **Responses Received with Error** - number of responses received that were in error.

show dhcp server counters

Displays various counters for the DHCP Server.

- Lease Requests Received
- Lease Accepts Received
- Lease Renewals Received
- Lease Refusals Received
- Lease Releases Received
- Unrecognized Packets Received
- Lease Offers Transmitted
- Lease Confirmations Transmitted
- Renewal Refusals Transmitted
- Lease Confirmations Transmitted
- Requested Address Out of Range
- Requested Address In Use
- No Free Addresses

show dhcp server settings

Displays the current settings for the DHCP Server.

- **Status** - Whether DHCP Server is active.
- **Start IP Address** - First IP address in the pool of IP addresses that will be handed out through DHCP.
- **End IP Address** - Last IP address in the pool of IP addresses that will be handed out through DHCP.
- **IP Mask** - IP network mask that applies to the pool of IP addresses being administered.
- **IP Router** - IP address that the workstations should use as their default gateway.
- **Lease** - The number of seconds that an IP address will be allocated to a workstation without having to be renewed.
- **Host Name** - DNS host name of this unit.
- **Domain Name** - Name of the DNS domain we exist in.

- **DNS #1** - IP address of the primary DNS server that the DHCP server will utilize when resolving names.
- **DNS #2** - IP address of the secondary DNS server that the DHCP server will utilize when resolving names.
- **WINS #1** - IP address of the primary WINS server that the DHCP server will utilize
- **WINS #2** - IP address of the secondary WINS server that the DHCP server will utilize.

show dns counters

Displays various counters for DNS.

- **Total Queries Received** - sum of DNS queries received
- **Total Response Sent** - sum of DNS responses sent
- **Responses from Local Processing** - number of DNS responses from local.
- **Responses from Remote Processing** - number of DNS responses from remote.
- **Success Responses** - successful responses to DNS requests
- **Error Responses** - sum of failures to DNS requests, specifics shown below

SPECIFIC ERROR COUNTERS

- **Format Errors** - server said invalid request format
- **Problems with Name Server** - internal server error
- **NonExistent Name** - number of times requested name could not be resolved
- **Server refused the request** - server was able to accept a request
- **Server does not implement request** - server was able to accept a request
- **Corrupted Responses** - response did not decrypt
- **Timeouts** - number of time outs waiting for the server to respond
- **Response could not be sent** - the requester had terminated

show dns settings

Displays settings for all DNS servers. You can modify using *set DNS*.

- **Administration Status** - This controls whether the DNS server has administration status. Options are Enabled or Disabled.
- **Number Retries per Server** - number of times the resolve name request will be sent to each Name Server, if the server fails to respond to a request before the timeout period
- **Timeout Period in Seconds** - number of seconds to wait before deciding a request to a Name Server has timed out

show filter <filter_name>

- **protocols [BR-ETH,BR-ETH-CALL,IP | IP-CALL, IP-RIP]**

Displays the filter rules, based on the protocol options specified. The filter name MUST be a filter file, as listed using *list filters*.

- **BR-ETH** - Ethernet bridge data filter rules

- **BR-ETH** - CALL - Ethernet bridge call filter rules
- **IP** - IP data filter rules
- **IP-CALL** - IP call filter rules
- **IP-RIP** - IP RIP advertisement filter rules

show icmp counters Shows the Input and Output Counters for ICMP. Two types of ICMP messages - error and query messages - are sent to syslog hosts.

ICMP COUNTERS

INPUT COUNTERS

- **Messages** - ICMP packets received.
- **Errors** - ICMP packets received with errors.
- **Destination Unreachable** - sum of ICMP messages received when a router cannot forward a packet to its specified destination
- **Time Exceeded** - sum of ICMP messages generated by a router when time has exceeded or a timeout has occurred while waiting for a packet segment
- **Parameter Problems** - sum of ICMP messages generated by a router when it encounters an error
- **Source Quench** - sum of ICMP messages informing a host it should slow data transmission to ease congestion
- **Redirects** - sum of ICMP messages concerning a router advertising a host of a better next hop
- **Echos** - sum of ICMP request messages received, signifying transport system success
- **Echo Replies** - sum of ICMP reply messages received, indicating transport system success
- **Timestamps** - sum of ICMP request messages received seeking time from another machine for clock synchronization and estimated transit time purposes
- **Timestamp Replies** - sum of ICMP timestamp reply messages
- **Address Masks** - sum of ICMP Address Mask Reply messages
- **Address Mask Replies** - sum of ICMP request messages concerning a host's ability to gather network information

OUTPUT COUNTERS

- **Messages** - total of ICMP messages transmitted
- **Errors** - ICMP packets transmitted with errors
- **Destination Unreachable** - sum of these messages sent
- **Time Exceeded** - sum of these messages sent
- **Parameter Problems** - sum of these messages sent
- **Source Quench** - sum of these messages sent
- **Redirects** - sum of these messages sent

- **Echos** - sum of ICMP Echo (request) messages sent
- **Echo Replies** - sum of these messages sent
- **Timestamps** - sum of these messages sent
- **Timestamp Replies** - sum of these messages sent
- **Address Masks** - sum of these messages sent
- **Address Mask Replies** - sum of these messages sent

show interface <interface_name> counters

Displays counters for the specified interface.

INPUT COUNTERS

- **Octets** - bytes received
- **Ucast** - Unicast packets received
- **MultiCast** - Multicast packets received
- **BroadCast** - broadcast packets received
- **Discards** - Number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
- **Errors** - For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a number of inbound transmission units that contained higher-layer protocol.
- **Unknown Prot** - unknown protocol in packet

OUTPUT COUNTERS

- **Octets** - bytes transmitted
- **Ucast** - unicast packets transmitted
- **MultiCast** - multicast packets transmitted
- **Discards** - Number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
- **Errors** - For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
- **Out QLen** - length of the output packet queue (in packets)

show interface <interface_name> settings

Displays settings for the specified interface. The settings displayed depend on the interface you specify, and so will not be shown here.

show ip counters

Displays system wide IP network statistics.

INPUT COUNTERS

- **Total Input Datagrams** - sum of IP datagrams received
- **Bad Headers** - number of datagrams with bad headers
- **Bad Addresses** - number of datagrams with bad addresses
- **Forwarded Packets** - number of packets forwarded
- **Bad Protocol** - number of packets received with bad protocol
- **Discarded** - number of packets discarded
- **Successfully Delivered** - number of packets successfully received

OUTPUT COUNTERS

- **Total Output Datagrams** - sum of datagrams transmitted
- **Discarded** - number of datagrams discarded
- **Bad Routes** - number of datagrams with a bad route
- **Fragments Needing Reassembly** - # of fragmented datagrams
- **Datagrams Successfully Reassembled** - # of broken datagrams successfully reassembled
- **Reassembly Failures** - # of broken datagrams unsuccessfully reassembled
- **Datagrams Successfully Fragmented** - datagrams successfully broken before transmission
- **Fragmentation Failures** - failed datagram fragmentations before transmission
- **Total Fragments** - sum of fragments transmitted

show ip settings

Displays system wide IP information.

- **IP Dynamic Address Pool Begin** - start of IP address range
- **IP Dynamic Address Pool Size** - size of IP address range
- **IP System Host Address** - IP address of the system
- **IP Forwarding** - ENABLE or DISABLE forwarding of IP packets

show ip network <network_name> settings

Displays parameter settings for the specified IP network. See the *set ip network* command on page 29 for additional details.

- **Interface** - interface this IP network runs on
- **Network Address** - network address of this IP network
- **Frame Type** - frame type used by the interface
- **Status** - ENABLED, ACTIVE, INACTIVE, DISABLED
- **Reconfigure Needed** - This is TRUE or FALSE.
- **Mask** - subnet mask used by this IP network
- **Station** - station address of this IP network

- **Broadcast Algorithm** - broadcast algorithm used for this network
- **Max Reassembly Size** - maximum packet size allowed to be reassembled from fragments
- **IP Routing Protocol** - routing protocol used
- **IP RIP Routing Policies** - routing policies used by RIP
- **IP RIP Authentication Key** - text string used for RIPv2 authentication

show ipx counters

Displays counters for all IPX network activity.

INPUT COUNTERS

- **Total Packets Received** - sum of IPX packets received
- **Header Errors** - sum of incoming packets discarded due to errors in their headers, including any IPX packet sized less than a minimum of 30 bytes
- **Unknown Sockets** - sum of incoming packets discarded because the destination socket was not open
- **Discarded** - sum of incoming packets discarded due to reasons other than those accounted for by Header Errors, and Unknown Sockets
- **Checksum Errors** - sum of IPX packets received with wrong checksums
- **Delivered Locally** - sum of IPX packets delivered locally, including packets from local applications
- **No Route to Destination** - number of times no route to a destination was found
- **Too Many Hops** - sum of incoming packets discarded for exceeding the hop count
- **Filtered Out** - sum of incoming packets filtered out
- **Decompression Errors** - sum of incoming packets discarded due to compression errors

OUTPUT COUNTERS

- **Total Packets Transmitted** - sum of IPX packets transmitted
- **Forwarded Packets** - sum of IPX packets forwarded
- **Local Transmits** - sum of IPX packets transmitted to local hosts
- **Local Malformed Transmits** -
- **Discarded** - sum of outgoing packets discarded
- **Filtered Out** - sum of packets filtered out before transmission
- **Compression Errors** - sum of outgoing packets discarded due to compression errors
- **Socket Open Failures** - sum of outgoing packets discarded because a socket was not available

show ipx network <network_name> counters

Displays statistics for the specified IPX network.

- **RIP Out Packets** - sum of RIP packets transmitted

- **RIP In Packets** - sum of RIP packets received
- **SAP Out Packets** - sum of SAP packets transmitted
- **SAP In Packets** - sum of SAP packets received

show ipx network <network_name> settings

Displays parameter settings for the specified IPX network. You can modify most of these values using the *set ipx network* command.

- **Interface** - interface this IPX network uses
- **Network Address** - network address of this IPX network
- **Frame Type** - frame type used by the interface (ETHERNET II, SNAP, or LOOPBACK)
- **Maximum Packet Size** - maximum allowable packet size for this IPX network. Default is 1500.
- **Status** - operational state of the network
- **Network Delay (ticks) -** time in number of ticks it takes to reach this IPX network
- **Network Learning Retries** - number of times this network will re-send packets to discover its directly connected neighbors
- **Diagnostics** - sending of diagnostic packets ENABLED or DISABLED
- **NetBIOS** - support ENABLED or DISABLED
- **NetBIOS Name Caching** - support ENABLED or DISABLED
- **NetBIOS Cache Timer (sec)** - interval a NetBIOS system will be kept in the cache
- **NetBIOS Maximum Hops** - most hops this network will make to locate a NetBIOS system
- **RIP** - RIP status
- **RIP Update (sec)** - number of seconds to wait before aging out RIP entries
- **RIP Age Multiplier** - number to multiply the rip_update_interval by, to obtain the value for aging out the entries in the RIP database
- **RIP Max Packet Size** - largest allowable size of a RIP packet
- **SAP** - SAP state
- **SAP Update (sec)** - number of seconds to wait before aging out SAP entries
- **SAP Age Multiplier** - number to multiply the *sap_update_interval* by, to obtain the value for the aging out entries in the SAP database
- **SAP Packet Size** - greatest allowable size of a SAP packet
- **SAP Nearest Server Reply** - SAP seeks nearest neighbors, YES or NO

show ipx rip

- **settings**
- **counters**

Displays information about RIP for IPX.

Parameter	Description
settings	Displays the state of the IPX routing. This is ON or OFF.
counters	Displays the **Incorrect RIP Packets** for the IPX routing. The incorrect RIP packets are the number of RIP packets that do not make sense.

show ipx sap

- **settings**
- **counters**

Displays information about SAP for IPX.

Parameter	Description
settings	Displays the state of the IPX routing. This is ON or OFF.
counters	Displays the **Incorrect SAP Packets** for the IPX routing. The incorrect SAP packets are the number of SAP packets that do not make sense.

show ipx settings Displays settings for dynamic IPX networks. You can modify these values using the *set ipx system* command.

- **Default Gateway** - default IPX router address
- **Max Open Sockets** - maximum allowed number of open sockets to remote IPX networks
- **Max Hops** - maximum allowed hops to remote IPX networks.
- **Priority** - preferred ranking of dynamic IPX networks
- **Dynamic Address Pool Begin** - starting IPX address
- **Dynamic Address Pool Size** - number of addresses to reserve for dynamic IPX address assignments

show memory Displays System DRAM Memory usage.

- **Total System Memory Resources** - total amount of memory in system
- **Free Memory** - amount of memory not in use
- **Code Size** - amount of memory used by code
- **Initialized Data Size**, **Uninitialized Data Size**, **Stack Size** - static data areas

show network <name> settings Displays the configured settings for the specified network. The display varies depending on the type of network specified. Some of the settings displayed are Interfaces, Network Address, Frame Type, Status, User Name, and Spawning Tree Enabled.

show network <name> counters Displays the statistical counters for the specified network. The display varies depending on the type of network specified. Some of the counters are Received Frames, Transmitted Frames, and Discarded Frames.

show ppp on vc <vc_name> counters

This shows counters for the Point-to-Point Protocol on the Virtual Circuit.

show ppp on vc <vc_name> settings

This shows the settings for the Point-to-Point Protocol on the Virtual Circuit.

show ppp on interface <name> counters

Displays statistics for PPP running on the specified interface.

COUNTERS for PPP BUNDLE 1

- **Operational Status** - *not opened* or *opened*
- **Number Active Links** - sum of active links using this PPP bundle
- **Transmit Packets** - sum of packets transmitted over this bundle
- **Bytes from Upper Layer** - sum of bytes received from an upper layer application for transmission over this bundle. This counter represents all data handed down to the PPP application BEFORE compression occurs.
- **Bytes to Lower Layer** - sum of bytes sent to a lower layer application for transmission over this bundle. This counter represents all data to be handed down to the lower layer application AFTER compression occurs.
- **Received Packets** - sum of packets received from a lower layer application over this bundle
- **Bytes to Upper Layer** - sum of bytes to be handed up to an upper layer application over this bundle
- **Bytes from Lower Layer** - sum of bytes received from a lower layer application over this bundle
- **Total Bad Headers** - sum of packets with incorrect PPP Header (Address, Control, PID Field)

COUNTERS for PPP LINK 1 - 5

- **Operational Status** - *not opened* or *opened*
- **Received Packets** - too long
- **Transmit Frames** - sum of frames received from the PPP application for transmission over this link
- **Bytes from Upper Layer** - sum of bytes handed down from an upper layer application for this link
- **Bytes to Lower Layer** - sum of bytes received from a lower layer application for this link
- **Received Frames** - sum of frames received on this link
- **Bytes to Upper Layer** - sum of bytes handed up to an upper layer application over this link
- **Bytes from Lower Layer** -sum of bytes received from a lower layer application over this link

show ppp on interface <name> settings

Displays the settings for PPP on the specified WAN interface.

SETTINGS for PPP BUNDLE 1

- **Operational Status** - *opened* or *not opened*
- **Number Active Links** - number of links active on this PPP bundle
- **User Profile** - user whose parameters were used in creating links
- **Local MMRU** - MRU the remote entity uses when sending packets to local PPP entity. Default: 1514
- **Remote MMRU** - MRU the local entity uses when sending packets to remote PPP entity. Default: 1514
- **Local Endpoint Class** - type of address used as the identifier
- **Local Endpoint Length** - maximum length of the local Endpoint Discriminator Address, default is 6
- **Local Endpoint ID** - value of the local Endpoint Discriminator Address
- **Remote Endpoint Class** - value of the remote Endpoint Discriminator Class, which indicates the type of address being used as the identifier
- **Remote Endpoint Length** - maximum length of the remote Endpoint Discriminator Address
- **Remote Endpoint ID** - value of the remote Endpoint Discriminator Address

SETTINGS for PPP BUNDLE 1 COMPRESSION
Operational Status - *Opened* or *Not Opened*

- **Compression Protocol** - authentication protocol used by the local PPP entity when it authenticated the local PPP entity to the remote PPP entity: PAP, CHAP or NONE

SETTINGS for PPP LINK 1 - 5

- **Operational Status** - *opened* or *not opened*
- **Interface Index** - index number of the interface used
- **Local MRU** - MRU the remote entity uses when sending packets to local PPP entity. Default: 1514
- **Remote MRU** - MRU the local entity uses when sending packets to remote PPP entity, default is 1514
- **Local to Peer ACC Map** - value of the ACC Map used for sending packets from the local PPP entity to the remote PPP entity
- **Peer to Local ACC Map** - ACC Map used by the remote PPP entity when transmitting packets to the local PPP entity
- **Local To Remote Protocol Compression** - Indicates whether the local PPP entity will use Protocol Compression when sending packets to the remote PPP entity. Default: ENABLED.
- **Remote To Local Protocol Compression** - Indicates whether the remote PPP entity will use Protocol Compression when transmitting packets to the local PPP entity. Default: ENABLED.
- **Local To Remote ACC Compression** - Indicates whether the local PPP entity will use Address and Control Compression when sending packets to the remote PPP entity. Default: ENABLED.

- **Remote To Local ACC Compression** - Indicates whether the remote PPP entity will use Address and Control Compression when sending packets to the local PPP entity. Default: ENABLED.

SETTINGS for PPP LINK 1 - 5 AUTHENTICATION

- **Operational Status** - *not opened* or *opened*
- **Local To Remote Compression Protocol** - authentication protocol used by the local PPP entity when it authenticated the itself to the remote PPP entity, PAP is the default
- **Remote To Local Compression Protocol** - authentication protocol used by the remote PPP entity when it authenticated the itself to the local PPP entity, PAP is the default

show ppp settings

Displays global settings for PPP. You can modify inbound authentication using the *set ppp receive_authentication* command.

- **Inbound Connections Authenticate PAP or CHAP** - Choices are: CHAP, PAP, EITHER or NONE. PAP is the default

show security_option settings

Displays status for SNMP User Access and Administration by Remote Users. You can modify the SNMP User Access using the *enable* or *disable security_option snmp* commands. You can modify Administration by Remote User using the *enable* or *disable security_option remote_user* commands.

- **SNMP User Access** - ENABLED (default) or DISABLED
- **Administration by Remote User** - ON or OFF

show snmp counters

Displays many SNMP statistics.

INPUT COUNTERS

- **Packets** - number of SNMP packets received
- **Bad Versions** - SNMP messages for an unsupported SNMP version
- **Bad Community Names** - SNMP messages which used an unknown SNMP community name
- **Bad Community Uses** - SNMP messages which represented an SNMP operation not allowed by the SNMP community named in the message
- **ASN.1 Parse Errors** - sum of ASN.1 or BER errors
- **Too Big Errors** - SNMP PDUs for which the value of the error-status field is tooBig'
- **No Such Name Errors** - SNMP PDUs where error-status field is `noSuchName'
- **Bad Value Errors** - SNMP PDUs where error-status field is `badValue'
- **Read Only Errors** - SNMP PDUs where the error-status field is `readOnly'
- **General Errors** - SNMP PDUs where the error-status field is `genErr'
- **Total Request MIB Objects** - sum of MIB objects retrieved successfully as the result of receiving valid SNMP Get-Request and Get-Next PDUs

- **Total Set MIB Objects** - sum of MIB objects altered successfully as the result of receiving valid SNMP Set-Request PDUs
- **Get Request PDUs** - sum of SNMP Get-Request PDUs accepted and processed
- **Get Next Request PDUs** - sum of SNMP Get-Next PDUs accepted and processed
- **Set Request PDUs** - sum of SNMP Get-Next PDUs accepted and processed
- **Get Response PDUs** - sum of SNMP Get-Response PDUs accepted and processed
- **Trap PDUs** - sum of SNMP Trap PDUs accepted and processed

OUTPUT COUNTERS

- **Packets** - sum of SNMP packets transmitted
- **Too Big Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `tooBig'
- **No Such Name Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `noSuchName'
- **Bad Value Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `badValue'
- **General Errors** - sum of SNMP PDUs generated by SNMP and for which the value of the error-status field is `genErr'
- **Get Request PDUs** - sum of SNMP Get-Request PDUs sent from SNMP
- **Get Next Request PDUs** - sum of SNMP Get-Next PDUs sent from SNMP
- **Set Request PDUs** - sum of SNMP Set-Request PDUs sent from SNMP
- **Get Response PDUs** - sum of SNMP Get-Response PDUs from SNMP
- **Trap PDUs** - sum of SNMP Trap PDUs sent from SNMP

show snmp settings Displays SNMP settings, which you can modify using *enable* or *disable snmp authentication traps* commands.

- **Authentication Traps** - ENABLED (default) or DISABLED

show system Displays system information.

- **System Descriptor** - for example:
  3Com OfficeConnect™ Remote 812 V1.0.0, Built on Oct 31 1998 at 11:33:05.
- **Object ID** - identifies this system to SNMP managers
- **System UpTime** - time the system has been running since last boot
- **System Contact** - modify using *set system*
- **System Name** - modify using *set system*
- **System Location** - modify using *set system*
- **System Services -** for example, Internet End To End Applications
- **System Version** - loaded version of the system software

show telnet Displays the status of the TELNET *escape* feature (ENABLED or DISABLED). It is set using the *disable* and *enable TELNET escape* commands.

show tcp counters Displays system-wide TCP statistics.

TCP COUNTERS

- **Active Opens** - number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state
- **Passive Opens** - number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state
- **Attempt Fails** - # of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state & the # of times TCP connections made a direct transition to the LISTEN state from the SYN-RCVD state
- **Resets** - # of times TCP connections made a direct transition to CLOSED state from either ESTABLISHED or CLOSE-WAIT states
- **Currently Established** - number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT
- **Input Segments** - sum of segments received
- **Output Segments** - sum of segments sent, including those on current connections but excluding those containing only retransmitted octets
- **Retransmitted Segments** - sum of segments retransmitted

show tcp settings Displays system-wide TCP settings.

TCP SETTINGS

- **Retransmission Algorithm** - for example, Van Jacobson
- **Minimum Timeout** - minimum retransmission timeout interval
- **Maximum Timeout** - maximum retransmission timeout interval
- **Maximum Connections** - sum of TCP connections allowed. If maximum number of connections is dynamic, the value is -1.

show tunnel Displays parameter values currently defined for the specified tunnel.

show udp Displays statistics for UDP datagrams.

INPUT COUNTERS

- **Total Input Datagrams** - sum of UDP datagrams received
- **Input but No Port** - sum of received UDP datagrams for which there was no application at the destination port
- **Input with other Errors** - sum of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port

OUTPUT COUNTERS

- **Total Output Datagrams** - sum of UDP datagrams sent.

show user <name> settings Displays the parameters defined for the specified TELNET user. You can use *list users* to see which users are defined.

show vc <vc_name> settings Displays the parameters defined for the specified VC. You can use *list vc* to see which virtual channels are defined.

TELNET

TELNET commands are available to users who dial in, and whose *type* is **network** (type parameter in *add user*), whose *host_type* is **prompt** (host_type parameter in *set login user*), and whose *login_service* is **TELNET** (login_service parameter in *set login user*).

telnet <ip_name_or_addr> Establishes a TELNET client session with the specified IP host name or address. In order for the system to resolve the host name, you must either add the host name and address to the DNS local host table, or define a DNS server.

telnet <ip_name_or_addr> TCP_port <number> Establishes a TELNET client session with the specified IP host name or address using the specified TCP port number. It works just like the TELNET command, except you also specify the TCP port number to be used. The default TCP port number is 23.

VERIFY

verify filter <filter_name> Verifies the syntax of a filter file, which has been previously *add*ed to the table. If you update a filter file and TFTP it to the FLASH file system, and the file already exists in the filter table, then you use this command to verify the files syntax. You can use *list filters* to see which files are currently in the filter file table, and what the status of each is.

TELNET Commands

The following commands are available to TELNET users. They are accessed by pressing control -].

close Closes the active TELNET connection.

help Lists the available commands

send <string> Transmits a TELNET control character. Be sure the parameters are *uppercase*. The choices are:

Parameter	Description
AYT	Are you there
IP	Interrupt process
BRK	Break
AO	abort output
EC	erase character
EL	erase line
GA	go ahead
NOP	no - operation

EOR	end of record
SYNC	synch

set_escape <string> Allows changing the TELNET escape character from **^]** to something else. Control characters are specified using the carat character followed by another character. For example, to set the TELNET escape character to control - X, type **set_escape ^X**.

status Displays the IP address of the remote host and the value of the TELNET escape character.

CLI Exit Commands

These commands are available to TELNET users so they can disconnect from the CLI.

Bye, Exit, Leave, Quit Leave the CLI, but keep this connection open.

This command returns you to the TELNET commands.

Logout Leave the CLI and close this connection. This ends the TELNET session.

Command Features

The command language has several built in features that make it easier to use. When abbreviating commands, it is sometimes hard to remember the commands and their syntax. Using command completion and positional help aids in jogging your memory of the commands and their parameters while you are typing in a command string.

Command Retrieval

Command retrieval retrieves commands from the *history* of previous commands entered. You can display the current command history using the *history* command. You can change the number of commands kept in the command history buffer using the *set command history* command.

^p	recall the previous command in the history list
^n	recall the next command in the history list

POSITIONAL HELP Positional help displays the list of possible parameters when you type **?** after any command or parameter. It then redisplays the line you typed, without the **?**, so you can enter the parameter you wish to use. This helps you find the parameter you need, and add it to your command, without having to retype the entire command string. Be sure to leave a space between the keyword and the question mark to use positional help.

Command Completion

The escape key provides command completion. If you press the escape key before you finish typing a command or parameter, the rest of the command or parameter will be displayed (completed), and you can continue entering the command. If the command or parameter is ambiguous, the bell will ding, and the display will not change.

Output Pause

The output will pause when there is more than 24 lines of output. Type ‘more’ (or press CR) to continue, or ‘quit’ to stop.

Command Kill

To discontinue the current command action, and flush any commands which have been typed ahead, use ^C (control-C).

Comments

; Nothing following the semicolon will be processed. This is useful when you are writing CLI script files. The *do* command runs a CLI script.

INDEX

3Com Corporation Limited Warranty

Hardware

3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Network interface cards	Lifetime
Other hardware products (unless otherwise specified in the warranty statement above)	1 year
Spare parts and spares kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

Software

3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. The sole obligation of 3Com with respect to this express warranty shall be (at the discretion of 3Com) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third-party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the noncompatibility is caused by a "bug" or defect in the third party's product.

Standard Warranty Service

Standard warranty service for *hardware* products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to the 3Com Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for *software* products may be obtained by telephoning the 3Com Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to the 3Com Corporate Service Center must be preauthorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at the expense of 3Com, not later than thirty (30) days after receipt of the defective product by 3Com.

Warranties Exclusive

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT THE OPTION OF 3COM. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

Limitation of Liability

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT THE OPTION OF 3COM. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law

This Limited Warranty shall be governed by the laws of the State of California, U.S.A. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. This warranty gives you specific legal rights which may vary depending on local law.

3Com Corporation, 5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (408) 764-5000

FCC Class A Verification Statement

WARNING: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, "Digital Apparatus," ICES-003. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment.

FCC Class B Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

WARNING: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, “Digital Apparatus,” ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from the one which the receiver is connected to.
- Consult the dealer or an experienced radio/TV technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

The Interference Handbook

This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-00345-4.

NOTE: In order to maintain compliance with the limits of a Class B digital device, 3Com requires that you use quality interface cables when connecting to this device. Changes or modifications not expressly approved by 3Com could void the user’s authority to operate this equipment. Refer to the manual for specifications on cabling types.

FCC Declaration of Conformity

We declare under our sole responsibility that the

Model:	**Description:**
	3Com OfficeConnect Remote 812 ADSL Router

to which this declaration relates, is in conformity with the following standards or other normative documents:

- ANSI C63.4-1992 Methods of Measurement

Federal Communications Commission 47 CFR Part 15, subpart B
3Com Corporation, 5400 Bayfront Plaza, P.O. Box 58145, Santa Clara, CA 95052-8145